Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Declaración de Seguridad

reducida de la

TARJETA DNIE 4.01

20 de mayo de 2024

Versión 1.0 Revisión 0

	NOMBRE	FECHA
Elaborado por:	Área de Desarrollo – Documentos de Identificación / Tarjetas	20/05/2024
Revisado por:		
Aprobado por:		

HISTÓRICO DEL DOCUMENTO				
Versión	**Revisión**	**Fecha**	**Descripción**	**Autor**
1.0	0	20/05/2024	Versión reducida	FNMT-RCM

Documento clasificado como: *Público*

Destinatarios: Departamento de Documentos de Identificación/Tarjetas de la FNMT-RCM, Centro Criptológico Nacional

Indice

1. Introducción

1.1. Identificación

1.1.1. Identificación de la declaración de seguridad

Título: Declaración de Seguridad reducida de la tarjeta DNIe 4.01

Nombre del fichero: Declaración de Seguridad reducida DNIe

Versión: 1.0.

Revisión: 0.

Autor: FNMT - Departamento de Documentos de Identificación – Tarjetas

Fecha: 20 de mayo de 2024

1.1.2. Identificación del objeto a evaluar (TOE)

TOE: DNIe

Versión: 4.01

Compuesto de:

IC plataforma subyacente:

Sistema Operativo: DNIe

Opciones:

- DNIe 05.52 A01 H 00B8
- DNIe 05.52 B01 H 00B8
- DNIe 05.52 C01 H 00B8
- DNIe 05.52 D01 H 00B8

1.2. Resumen

Esta declaración de seguridad establece las bases para la evaluación Common Criteria [CC] de la tarjeta “DNI electrónico” en su versión y opciones identificadas anteriormente.

The TOE type addressed by the current security target is a smartcard programmed according to [TR03110-2]. The programmed smartcard is called an electronic document as a whole. Here, an application is a collection of data(groups) and their access conditions. We mainly distinguish

between common user data, and sensitive user-data. Depending on the protection mechanisms involved, these user data can further be distinguished as follows:

1. EAC1-protected data: Sensitive user data protected by EAC1,
2. EAC2-protected data: Sensitive user data protected by EAC2, and
3. all other (common) user data. Other user data are protected by Password Authenticated Connection Establishment (PACE]). Note that EAC1 recommends, and EAC2 requires prior execution of PACE.

In addition to the above user data, there are also data required for TOE security functionality (TSF). Such data is needed to execute the access control protocols, to verify integrity and authenticity of user data, or to generate cryptographic signatures.

The TOE contains the following applications and protocols:

- Electronic Document configuration: user data contained in [TR03110-2]-conformant eID, and eSign applications. An ePass/MRTD/Residence Permit[3] application is included as well, but it is compliant to [ICAO9303] in order to be an EU-compliant MRTD application. User data of eSign and eID applications are protected by PACE/EAC2; whereas on the ePass application, user data is protected by PACE/EAC1/EAC2.

This ST claims strict conformance to [PACEPP], [EAC1PP] and [EAC2PP]. There, slightly different terminology is used. For the ease of understanding, **Tabla 1** gives the equivalence between the used terminology in this ST and the different PPs, as in some parts of this document the original terminology of each PP is also conserved.

This ST	PACE PP	EAC1PP	EAC2PP
electronic document	travel document	travel document	electronic document
electronic document presenter	traveler	traveller	electronic document presenter
EAC1 protected data	-	sensitive (user) data	-
EAC2 protected data	-	-	sensitive user data
common user data	user data	user data	common user data
PACE terminal	BIS-PACE	BIS-PACE	PACE terminal
EAC1 terminal	-	Extended Inspection System	-
EAC2 terminal	-	-	EAC2 terminal

Tabla 1.- Overview of identifiers of this ST and claimed PPs.

De aquí en adelante, al TOE se le denominará indistintamente “DNI electrónico”, “DNIe”, “tarjeta DNIe”, “electronic document”, “travel document” o simplemente “tarjeta”.

[3] ePass/MRTD/Residence Permit applications. All references to ePass application should be understood as ePass/MRTD/Residence Permit applications. From the TOE point of view are the same application, the only diference between them is the physical material which is not part of the TOE and holds the IC (booklet or card).

1.2.1. Non-TOE Hardware/Software/Firmware

No existe un hardware, software o firmware específico requerido por el TOE para llevar a cabo las características de seguridad que declara. El TOE se define compuesto por el chip y el sistema operativo del TOE. En cualquier caso, se debe tener en cuenta que el soporte plástico que contiene el chip así como la antena son necesarios para representar un documento de identidad y viaje completo, aunque estas partes no son imprescindibles para llevar a cabo las operaciones seguras del TOE.

1.3. Descripción del TOE

Como se ha indicado en el apartado "Identificación del objeto a evaluar (TOE)", el TOE está compuesto por: un controlador de seguridad (chip) y un sistema operativo (DNIe, versión 5.52). También se incluyen los manuales que contienen los procedimientos de operación e instalación:

Documento	**Referencia**
Guía preparativa. DNIe 4.01. v1.0 r0. 20/05/24.	[GP]
Guía operativa para usuario final. DNIe 4.01. v1.0 r0. 20/05/24.	[GOU]
Guía operativa para administrador. DNIe 4.01. v1.0 r0. 20/05/24.	[GOA]
Guías Operativas. DNIe 4.01. v1.0 r0. 20/05/24	[GO]
Anexo I Ejemplo - Guía Operativa para usuario final. DNIe 4.01 v1.0 r0. 20/05/24.	[AGO]
Especificación funcional. Manual de comandos. DNIe 4.01. v1.0 r0. 20/05/24.	[CMD]
Scripts de expedición: • DNIe_5_52_Expedicion_CerrarDNIe_v01 • DNIe_5_52_Expedicion_ePassport_v01 • DNIe_5_52_Expedicion_eID_v01 • DNIe_5_52_Expedicion_eSign_v01	-

El TOE se entrega encartado en una tarjeta física con el diseño gráfico y medidas de seguridad a la DGP cliente por parte de la FNMT-RCM. Las tarjetas se agrupan y se almacenan en su embalaje correspondiente (típicamente contenedores o cajas de cartón) y se empaquetan agrupados por lotes que se entregan físicamente en la oficina que la DGP tiene en las instalaciones de la FNMT-RCM. De forma adicional se entregan por correo los documentos y scripts de la tabla anterior cifrados y en formato pdf, para su validación conforme a las especificaciones y requisitos del producto.

El conjunto de todos ellos conforma un TOE con las funciones de seguridad que a lo largo de este apartado se detallan.

Los elementos controlador de seguridad y librería criptográfica, ya han sido evaluados y certificados por su fabricante. Los resultados de estas certificaciones se emplean para realizar la evaluación compuesta del TOE, conforme a los requisitos del documento [ASE_COMP].

The TOE contains the following applications and protocols:

- Electronic Document configuration: user data contained in [TR03110-2]-conformant eID, and eSign applications. An ePass/MRTD/Residence Permit4 application is included as well, but it is compliant to [ICAO9303] in order to be an EU-compliant MRTD application. User data of eSign and eID applications are protected by PACE/EAC2; whereas on the ePass application, user data is protected by PACE/EAC1 and EAC2.

The purpose and usage of the above mentioned different applications is as follows:

- An eID application, as defined in [TR03110-2], including related user data and data needed for authentication, is intended to be used for accessing official and commercial services which require access to user data stored in the application. For the eID application, the electronic document holder can control access to his user data by inputting his secret PIN or by consciously presenting his electronic document to authorities;

- An eSign application, as defined in [TR03110-2], is intended to generate qualified electronic signatures. The main specific property distinguishing qualified electronic signatures from other, i.e. advanced electronic signatures, is that they are based on qualified certificates and created by secure signature creation devices (SSCD). For the eSign application, the electronic document holder can control access to the digital signature functionality by consciously presenting his electronic document to an EAC2 terminal and inputting his secret PIN for this application.

- An ePass application, compliant to [ICAO9303] since user data is protected by PACE/EAC1 and EAC2, supports Passive Authentication, Password Authenticated Connection Establishment (PACE) with CAN and MRZ as parts of the Standard and General Inspection Procedure, Terminal and Chip Authentication version 1.

Each application contains its own set of user data, composed according to its requirements.

Application note 1: While it is technically possible to grant access to the electronic signature functionality by inputting only the CAN (see [TR03110-2]), this technical option is not allowed by the security policy defined for the eSign application. This is due to the fact that solely the

[4] ePass/MRTD/Residence Permit applications. All references to ePass application should be understood as ePass/MRTD/Residence Permit applications. From the TOE point of view are the same application, the only diference between them is the physical material which is not part of the TOE and holds the IC (booklet or card).

signatory – which is here the electronic document holder – shall be able to generate an electronic signature on his own behalf.

Application note 2: The cryptographic algorithms used by the TOE are defined outside the TOE in the Public Key Infrastructure. The security parameters of these algorithms must be selected by the electronic document issuer according to the Organizational Security Policies. The TOE supports the standardized domain parameters mentioned in [RFC5639] (key length 256, 384 and 512 bit) related with curves (brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1), and also supports the following NIST curves (P-256, P-384 and P-521). PACE and hence the General Inspection Procedure require the use of AES-192. This depends on the Initialization of the TOE.

Operational use of the TOE is explicitly in the focus of current ST. Nevertheless, some TOE functionality might not be directly accessible to the end-user during operational use. Some single properties of the manufacturing and the card issuing life cycle phases that are significant for the security of the TOE in its operational phase are also considered by the current ST. Conformance with this ST requires that all life cycle phases are considered to the extent that is required by the assurance package chosen here for the TOE.

The following TOE security features are the most significant for its operational use. The TOE ensures that

- only authenticated terminals can get access to the user data stored on the TOE and use security functionality of the electronic document according to the access rights of the terminal,
- the electronic document holder can control access by consciously presenting his electronic document and/or by entering his secret PIN,
- authenticity and integrity of user data can be verified,
- confidentiality of user data in the communication channel between the TOE and the connected terminal is provided,
- inconspicuous tracing of the electronic document is averted,
- its security functionality and the data stored inside are self-protected, and
- digital signatures can be created.

The TOE also provides the following functions:

- to generate signature creation data (SCD) and the correspondent signature-verification data (SVD),
- to export the SVD for certification,
- to, optionally, receive and store certificate info,
- to switch the TOE from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps:
    - select an SCD if multiple are present in the SSCD,
    - authenticate the signatory and determine its intent to sign,
    - receive data to be signed or a unique representation thereof (DTBS/R),

- apply an appropriate cryptographic signature creation function using the selected SCD to the DTBS/R.

1.4. Ciclo de vida

The TOE life cycle is described in terms of the above mentioned four life cycle phases. Akin to [ICPP], the TOE life-cycle is additionally subdivided into seven steps.

Phase 1: Development

Step 1

The TOE is developed in phase 1. The IC developer develops the integrated circuit, the IC dedicated software and the guidance documentation associated with these TOE components.

Step 2

The software developer uses the guidance documentation for the integrated circuit and the guidance documentation for relevant parts of the IC dedicated software, and develops the IC embedded software (operating system), the electronic document application(s) and the guidance documentation associated with these TOE components.

The manufacturing documentation of the IC including the IC dedicated software and the embedded software in the non-volatile non-programmable memories is securely delivered to the IC manufacturer. The IC embedded software in the non-volatile programmable memories, the application(s), and the guidance documentation is securely delivered to the electronic document manufacturer.

Phase 2: Manufacturing

Step 3

In a first step, the TOE integrated circuit is produced. The circuit contains the electronic document's chip dedicated software, and the parts of the electronic document's chip embedded software in the non-volatile non-programmable memory (ROM). The IC manufacturer writes IC identification data onto the chip in order to track and control the IC as dedicated electronic document material during IC manufacturing, and during delivery to the electronic document manufacturer. The IC is securely delivered from the IC manufacturer to the electronic document manufacturer. If necessary, the IC manufacturer adds parts of the IC embedded software in the non-volatile programmable memory, e. g. EEPROM.

Step 4 (optional)

If the electronic document manufacturer delivers a packaged component, the IC is combined with hardware for the contactless interface.

Step 5

The electronic document manufacturer

1. if necessary, adds the IC embedded software, or parts of it in the non-volatile programmable memories, e. g. EEPROM or FLASH,
2. creates the application(s), and
3. equips the electronic document's chip with pre-personalization data.

Creation of the application(s) implies the creation of the master file (MF), dedicated files (DFs), and elementary files (EFs) according to [ISO7816-4]. How this process is handled internally depends on the IC and IC embedded software.

The pre-personalized electronic document together with the IC identifier is securely delivered from the electronic document manufacturer to the personalization agent. The electronic document manufacturer also provides the relevant parts of the guidance documentation to the personalization agent.

Phase 3: Personalization of the Electronic Document

Step 6

The personalization of the electronic document includes

1. the survey of the electronic document holder’s biographical data,
2. the enrollment of the electronic document holder's biometric reference data, such as a digitized portrait or other biometric reference data,
3. printing the visual readable data onto the physical part of the electronic document, and
4. configuration of the TSF, if necessary.

Configuration of the TSF is performed by the personalization agent and includes, but is not limited to, the creation of the digitized version of the textual, printed data, the digitized version of e.g. a portrait, or a cryptographic signature of a cryptographic hash of the data that are stored on the chip. The personalized electronic document, if required together with appropriate guidance for TOE use, is handed over to the electronic document holder for operational use.

Application note 3: TSF data are data for the operation of the TOE upon which the enforcement of the SFRs relies CC Part 1 [CC]. Here TSF data include, but are not limited to, the personalization agent's authentication key(s).

Phase 4: Operational Use

Step 7

The chip of the TOE is used by the electronic document and terminals that verify the chip's data during the phase operational use. The user data can be read and modified according to the security policy of the issuer.

The TOE additionally has the ability to update its TOE software during the life-cycle phase operational use by a secure update mechanism. The updated TOE software is out of scope of this ST as it will be a different version of the TOE.

Phase 5: End of life

Step 8

The TOE reaches its end of life and it is no longer valid.

2. Declaraciones de conformidad

2.1. Declaración de conformidad respecto a los Criterios Comunes

Esta declaración de seguridad declara conformidad con la norma [CC]:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017. Se declara conformidad extendida con esta parte.
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017. Se declara conformidad con esta parte.

Al ser un TOE compuesto, también se referencia la declaración de seguridad de la plataforma sobre la que se levanta el producto.

2.2. Declaración de conformidad respecto a otros PP

Esta declaración de seguridad declara conformidad estricta con los siguientes perfiles de protección [SSCDPP], [SSCDPP4], [SSCDPP5], [EAC1PP] y [EAC2PP]:

- Protection profiles for secure signature creation device – Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.0.1, 2012-01, BSI-CC-PP-0059-2009-MA-01, [SSCDPP].

- Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, prEN 14169-4:2012 ver. 1.0.1, 2012-11, BSI-CC-PP-0071. [SSCDPP4].
- Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application, prEN 14169-5:2012 ver. 1.0.1, 2012-11, BSI-CC-PP-0072. [SSCDPP5].
- Common Criteria Protection Profile — Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), ver. 1.3.2, 05th December 2012, BSI-CC-PP-0056-V2-2012. [EAC1PP].
- Common Criteria Protection Profile — Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110 (EAC2_PP), ver. 1.01, May 20th, 2015, BSI-CC-PP-0086. [EAC2PP].

Puesto que los dos últimos perfiles de protección [EAC1PP] Y [EAC2PP] declaran a su vez conformidad estricta con el perfil de protección [PACEPP], esta declaración de seguridad también declara de forma implícita conformidad estricta con dicho perfil de protección:

- Common Criteria Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.01, 22th July 2014, BSI-CC-PP-0068-V2-2011-MA-01. [PACEPP].

En resumen, esta declaración de seguridad cumple estrictamente el paquete de garantía EAL4 aumentado con los componentes ALC_DVS.2, ATE_DPT.2 y AVA_VAN.5 definidos en:

- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements; Version 3.1, Revision 5, April 2017.

2.3. Conformidad con eIDAS

Además del cumplimiento de los requisitos en la funcionalidad de firma electrónica, en relación a la funcionalidad de autenticación del ciudadano, el DNIe v4.01 cumple con los requisitos del Reglamento (UE) nº 910/2014 (eIDAS) en materia de identificación electrónica, requisitos derivados del Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015 sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3 del Reglamento eIDAS, en concreto los relativos a la Gestión de medios de identificación electrónica, autenticación, controles técnicos, cumplimiento y auditoría con niveles de seguridad ALTO.

También cumple con los requisitos derivados de la Decisión de Ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2 del Reglamento eIDAS.

2.4. Justificación de conformidad

El TOE presentado en esta declaración de seguridad se ajusta al tipo de objeto definido en [SSCDPP], [SSCDPP4], [SSCDPP5], [EAC1PP] y [EAC2PP] y [PACEPP], definido como documento electrónico que contiene las aplicaciones de firma electrónica, identidad digital y pasaporte electrónico.

Se deduce del análisis del contenido y de la presentación de las evidencias, que se satisfacen los requisitos del nivel de evaluación exigido, esto es, EAL4+ aumentado con ALC_DVS.2, ATE_DPT.2 y AVA_VAN.5.

La definición del problema de seguridad, los objetivos y requisitos de seguridad son consistentes con los presentados en los perfiles de protección [SSCDPP], [SSCDPP4], [SSCDPP5], [EAC1PP] y [EAC2PP] y [PACEPP] cumpliendo la conformidad estricta.

3. Compatibilidad entre aplicaciones del TOE

Con objeto de asegurar la compatibilidad de las diferentes aplicaciones presentes en el TOE (firma, identidad y documento de viaje), se ha tenido en cuenta el enfoque realizado por el perfil de protección:

- Common Criteria Protection Profile — Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use [MR.ED-PP], BSI-CC-PP-0087-V2-MA-01, Version 2.0.3, July 18th, 2016.

Sin embargo, esta declaración de seguridad no declara formalmente conformidad con dicho perfil de protección puesto que el TOE no implementa los protocolos de identificación restringida (Restricted Identification), firma pseudónima (Pseudonymous Signature) y autenticación de chip versión 3 (Chip Authentication 3) de la especificación técnica TR-03110 [TR03110-2].

Del mismo modo, en lo referente al mecanismo de actualización del TOE, esta declaración de seguridad sigue las recomendaciones descritas en el perfil de protección modular:

- Common Criteria Protection Profile - Configuration Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates) [MR.ED-ON-PP], BSI-CC-PP-0090-2016, Version 0.9.2, August 18th, 2016.

No obstante, tampoco se declara formalmente conformidad con dicho perfil de protección modular al estar definido éste sobre la base del perfil de protección [MR.ED-PP].

4. Security problem definition

4.1. Introduction

4.1.1. Assets

4.1.1.1. Primary assets

As long as they are in the scope of the TOE, the primary assets to be protected by the TOE are listed below. For a definition of terms used, but not defined here, see the Glossary.

Authenticity of the Electronic Document's Chip

The authenticity of the electronic document's chip personalized by the issuing state or organization for the electronic document holder, is used by the electronic document presenter to prove his possession of a genuine electronic document.

Generic Security Property: Authenticity

This asset is equal to the one(s) of [EAC1PP] and [EAC2PP], which itself stem from [PACEPP].

Electronic Document Tracing Data

Technical information about the current and previous locations of the electronic document gathered unnoticeable by the electronic document holder recognizing the TOE not knowing any PACE password. TOE tracing data can be provided / gathered.

Generic Security Property: Unavailability

This asset is equal to the one(s) of [EAC1PP] and [EAC2PP], which itself stem from [PACEPP]. Note that unavailability here is required for anonymity of the electronic document holder.

Sensitive User Data

User data, which have been classified as sensitive data by the electronic document issuer, e. g. sensitive biometric data. Sensitive user data are a subset of all user data, and are protected by EAC1, EAC2, or both.

Generic Security Properties: Confidentiality, Integrity, Authenticity

User Data stored on the TOE

All data, with the exception of authentication data, that are stored in the context of the application(s) on the electronic document. These data are allowed to be read out, used or modified either by a PACE terminal, or, in the case of sensitive data, by an EAC1 terminal or an EAC2 terminal with appropriate authorization level.

Generic Security Properties: Confidentiality, Integrity, Authenticity

This asset is included from [EAC1PP], [EAC2PP] respectively. In these protection profiles it is an extension of the asset defined in [PACEPP]. This asset also includes ”SVD” (Integrity and Authenticity only), “SCD” of [SSCDPP].

User Data transferred between the TOE and the Terminal

All data, with the exception of authentication data, that are transferred (both directions) during usage of the application(s) of the electronic document between the TOE and authenticated terminals.

Generic Security Properties: Confidentiality, Integrity, Authenticity

This asset is included from [EAC1PP], [EAC2PP] respectively. In these protection profiles it is an extension of the asset defined in [PACEPP]. As for confidentiality, note that even though not each data element being transferred represents a secret, [TR03110-1], [TR03110-2] resp. require confidentiality of all transferred data by secure messaging in encrypt-then-authenticate mode. This asset also includes “DTBS” and “DTBS/R” of [SSCDPP].

4.1.1.2. Secondary assets

In order to achieve a sufficient protection of the primary assets listed above, the following secondary assets also have to be protected by the TOE.

Accessibility to the TOE Functions and Data only for Authorized Subjects

Property of the TOE to restrict access to TSF and TSF-Data stored in the TOE to authorized subjects only.

Generic Security Property: Availability

Genuineness of the TOE

Property of the TOE to be authentic in order to provide claimed security functionality in a proper way.

Generic Security Property: Availability

Electronic Document Communication Establishment Authorization Data

Restricted-revealable authorization information for a human user being used for verification of the authorization attempts as an authorized user (PACE password). These data are stored in the TOE, and are not send to it.

Restricted-revealable here refers to the fact that if necessary, the electronic document holder may reveal her verification values of CAN and MRZ to an authorized person, or to a device that acts according to respective regulations and is considered trustworthy.

Generic Security Properties: Confidentiality, Integrity

Secret Electronic Document Holder Authentication Data

Secret authentication information for the electronic document holder being used for verification of the authentication attempts as authorized electronic document holder (PACE passwords).

Generic Security Properties: Confidentiality, Integrity

TOE internal Non-Secret Cryptographic Material

Permanently or temporarily stored non-secret cryptographic (public) keys and other non-secret material used by the TOE in order to enforce its security functionality.

Generic Security Properties: Integrity, Authenticity

TOE internal Secret Cryptographic Keys

Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.

Generic Security Properties: Confidentiality, Integrity

Application note 4: The above secondary assets represent TSF and TSF-Data in the sense of CC.

4.1.1.2.1. Secondary assets from [MR.ED-ON-PP]

Secret Cryptographic Update Keys

All cryptographic key material related to the update mechanism; i.e. cryptographic material that is used to establish a secure communication channel with the update terminal, to authenticate an update terminal, to decrypt and verify the authenticity of an update package, and for other update-related cryptographic operations. Note that this term deliberately includes public (in the cryptographic sense) signing keys installed on the TOE for verifying the authenticity of update packages, as well as ephemeral keys.

Meta-Data

Data that contains information about the update, e.g. version information, checksums, information w.r.t. applicability to specific product versions and platforms, etc.

Update Data

Unencrypted data that is used to update the TOE software.

Note that we use the term *update data* to denote the unencrypted data. Encrypted update data, appended with optional additional unencrypted meta-data (i.e. version number, TOE product identifier), and signed, is called an *update package*.

Update Log Data

Log records that store information about previously applied updates and failed update attempts.

Update Package

Encrypted update data, appended with optional unencrypted meta-data, and signed.

Update Package Verification Status

Security attribute indicating whether the supplied update was successfully verified (and where hence its authenticity and integrity can be assumed) or not, and whether an attempt to verify was made or not. Allowed values are NOT VERIFIED, SUCCESSFULLY VERIFIED and VERIFICATION FAILED.

Version Information

Version information that uniquely identify the version of the TOE software currently installed on the TOE.

4.1.2. Subjects

This security target considers the following external entities and subjects:

Attacker

A threat agent (a person or a process acting on his behalf) trying to undermine the security policy defined by the current ST, especially to change properties of the assets that have to be maintained. The attacker is assumed to possess at most high attack potential. Note that the attacker might capture any subject role recognized by the TOE.

Country Signing Certification Authority (CSCA)

An organization enforcing the policy of the electronic document issuer, i. e. confirming correctness of user and TSF data that are stored within the electronic document. The CSCA represents the country specific root of the public key infrastructure (PKI) for the electronic document, and creates Document Signer Certificates within this PKI. The CSCA also issues a self-signed CSCA certificate that has to be distributed to other countries by secure diplomatic means, see [ICAO9303].

Country Verifying Certification Authority (CVCA)

The Country Verifying Certification Authority (CVCA) enforces the privacy policy of the issuing state or organization, i. e. enforcing protection of sensitive user data that are stored in the electronic document. The CVCA represents the country specific root of the PKI of EAC1 terminals, EAC2 terminals respectively, and creates Document Verifier Certificates within this PKI. Updates of the public key of the CVCA are distributed as CVCA Link-Certificates.

Document Signer (DS)

An organization enforcing the policy of the CSCA. A DS signs the Document Security Object that is stored on the electronic document for Passive Authentication. A Document Signer is authorized by the national CSCA that issues Document Signer Certificate, see [ICAO9303]. Note that this role is usually delegated to a Personalization Agent.

Document Verifier (DV)

An organization issuing terminal certificates as a Certificate Authority, authorized by the corresponding CVCA to issue certificates for EAC1 terminals, EAC2 terminals respectively, see [TR03110-3].

Electronic Document Holder

A person the electronic document issuer has personalized the electronic document for. Personalization here refers to associating a person uniquely with a specific electronic electronic document. This subject includes “Signatory” as defined [SSCDPP].

Electronic Document Presenter

A person presenting the electronic document to a terminal and claiming the identity of the electronic document holder. Note that an electronic document presenter can also be an attacker. Moreover, this subject includes “user” as defined in [SSCDPP].

Manufacturer

Generic term comprising both the IC manufacturer that produces the integrated circuit, and the electronic document manufacturer that creates the electronic document and attaches the IC to it. The manufacturer is the default user of the TOE during the manufacturing life cycle phase. When referring to the role manufacturer, the TOE itself does not distinguish between the IC manufacturer and the electronic document manufacturer.

PACE Terminal

A technical system verifying correspondence between the password stored in the electronic document and the related value presented to the terminal by the electronic document presenter. A PACE terminal implements the terminal part of the PACE protocol and authenticates itself to the electronic document using a shared password (CAN, eID-PIN, eID-PUK or MRZ). A PACE terminal is not allowed reading sensitive user data.

Personalization Agent

An organization acting on behalf of the electronic document issuer that personalizes the electronic document for the electronic document holder. Personalization includes some or all of the following activities: (i) establishing the identity of the electronic document holder for the biographic data in the electronic document, (ii) enrolling the biometric reference data of the electronic document holder, (iii) writing a subset of these data on the physical electronic

document (optical personalization) and storing them within the electronic document's chip (electronic personalization), (iv) writing document meta data (i. e. document type, issuing country, expiry date, etc.) (v) writing the initial TSF data, and (vi) signing the Document Security Object, and the elementary files EF.CardSecurity and the EF.ChipSecurity (if applicable [ICAO9303], [TR03110-3]) in the role DS. Note that the role personalization agent may be distributed among several institutions according to the operational policy of the electronic document issuer. This subject includes “Administrator” as defined in [SSCDPP].

EAC1 Terminal / EAC2 Terminal

A terminal that has successfully passed the Terminal Authentication protocol (TA) version 1 is an EAC1 terminal, while an EAC2 terminal needs to have successfully passed TA version 2. Both are authorized by the electronic document issuer through the Document Verifier of the receiving branch (by issuing terminal certificates) to access a subset or all of the data stored on the electronic document.

Terminal

A terminal is any technical system communicating with the TOE through the contactless interface. The role terminal is the default role for any terminal being recognized by the TOE as neither being authenticated as a PACE terminal nor an EAC1 terminal nor an EAC2 terminal.

Users

This ST considers the following users and subjects acting for users:

- User: End user of the TOE that can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role of R.Admin or as S.Sigy in the role of R.Sigy.
- Administrator: User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.
- Signatory: User who hold the TOE and uses it on his own behalf or on behalf of the natural or legal person or entity he represents. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

4.1.2.1.1. Subject from [MR.ED-ON-PP]

Update Terminal

A terminal to read out version information and update log data of the TOE software, and to install updates of the TOE software. Prior executing these functions, the update terminal must authenticate itself towards the TOE.

4.2. Threats

This section describes the threats to be averted by the TOE independently or in collaboration with its IT environment. These threats result from the assets protected by the TOE and the method of the TOE's use in the operational environment.

4.2.1. Threats from [MR.ED-PP]

This section includes the following threats from [MR.ED-PP].

- **T.InconsistentSec** **Inconsistency of security measures**

  Adverse action: An attacker gains read or write access to user data or TOE data without being allowed to, due to an ambiguous/unintended configuration of the TOE's internal access conditions of user or TSF data. This may lead to a forged electronic document or misuse of user data.

  Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents.

  Asset: authenticity, integrity and confidentiality of user data stored on the TOE.

- **T.Interfere** **Interference of security protocols**

  Adverse action: An attacker uses an unintended interference of implemented security protocols to gain access to user data.

  Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents.

  Asset: authenticity, integrity and confidentiality of user data stored on the TOE.

4.2.2. Threats from [MR.ED-ON-PP]

- **T.FaTSF** **Faulty TSF**

  Adverse action: An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF, for example due to:

  - software issues that were not detected, not exploitable, or deemed unable to being exploitable at the time of certification, but due to unforeseen advances in technology became a security risk during operational use of the TOE, or

- cryptographic mechanisms that were deemed secure at the time of certification, but due to unforeseen advances in the field of cryptography became a security risk during operational use of the TOE.

Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

Asset: all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data)

- **T.UaU** **Unauthorized Update**

Adverse action: An attacker gains read or write access to user data or TSF data, or manipulates or mitigates the TSF by misuse of the update functionality. This threat contains two main aspects:

- the unauthorized installation, which may lead to the use of untimely, outdated or revoked updates.
- the installation of updates that are not authorized and authentic.

Threat agent: having high attack potential, being in possession of one or more legitimate electronic documents

Asset: all data stored on the TOE (esp. the integrity, authenticity and – if applicable – secrecy of the data).

4.2.3. Threats from [EAC1PP]

This section includes the following threats from [EAC1PP]. They concern EAC1-protected data.

- **T.Counterfeit** **Counterfeit of travel document chip data**

Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a genuine travel document's chip to be used as part of a counterfeit travel document. This violates the authenticity of the travel document's chip used for authentication of a traveller by possession of a travel document.
The attacker may generate a new data set or extract completely or partially the data from a genuine travel document's chip and copy them to another appropriate chip to imitate this genuine travel document's chip.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents.

Asset: authenticity of user data stored on the TOE.

- **T.Read_Sensitive_Data** **Read the sensitive biometric reference data**

  Adverse action: An attacker tries to gain the sensitive biometric reference data through the communication interface of the travel document's chip.

  The attack T.Read_Sensitive_Data is similar to the threat T.Skimming (cf. [BACPP]) in respect of the attack path (communication interface) and the motivation (to get data stored on the travel document's chip) but differs from those in the asset under the attack (sensitive biometric reference data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods. Note, that the sensitive biometric reference data are stored only on the travel document's chip as private sensitive personal data whereas the MRZ data and the portrait are visually readable on the physical part of the travel document as well.

  Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate travel document.

  Asset: confidentiality of logical travel document sensitive user data (i.e. biometric reference).

4.2.4. Threats from [EAC2PP]

This section includes the following threats from the [EAC2PP]. They concern EAC2-protected data.

- **T.Counterfeit/EAC2** **Counterfeit of electronic document chip data**

  Adverse action: An attacker with high attack potential produces an unauthorized copy or reproduction of a chip of a genuine electronic document. This copy or reproduction can be used as a part of a counterfeit electronic document. This violates the authenticity of the electronic document's chip used for

authentication of a electronic document presenter by possession of an electronic document. The attacker may generate a new data set or extract completely or partially the data from a genuine electronic document's chip and copy them to another appropriate chip to imitate the chip of the genuine electronic document.

Threat agent: having high attack potential, being in possession of one or more legitimate ID-Cards.

Asset: authenticity of user data stored on the TOE.

- **T.Sensitive_Data** **Unauthorized access to sensitive user data**

Adverse action: An attacker tries to gain access to sensitive user data through the communication interface of the electronic document's chip.The attack T.Sensitive_Data is similar to the threat T.Skimming from [PACEPP] w.r.t. the attack path (communication interface) and the motivation (to get data stored on the electronic document's chip) but differs from those in the asset under the attack (sensitive data vs. digital MRZ, digitized portrait and other data), the opportunity (i.e. knowing the PACE Password) and therefore the possible attack methods.

Threat agent: having high attack potential, knowing the PACE Password, being in possession of a legitimate electronic document.

Asset: confidentiality of sensitive user data stored on the electronic document.

4.2.5. Threats from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP], and thus include the threats formulated in [PACEPP]. We list each threat only once here.

- **T.Abuse-Func** **Abuse of Functionality**

Adverse action: An attacker may use functions of the TOE which shall not be used in TOE operational phase in order (i) to manipulate or to disclose the *User Data stored in the TOE*, (ii) to manipulate or to disclose the *TSF-data stored in the TOE* or (iii) to manipulate (bypass, deactivate or modify) *soft-coded security functionality*

of the TOE. This threat addresses the misuse of the functions for the initialisation and personalisation in the operational phase after delivery to the travel document holder.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document

- **T.Eavesdropping** **Eavesdropping on the communication between the TOE and the PACE terminal**

Adverse action: An attacker is listening to the communication between the travel document and the PACE authenticated BIS-PACE in order to gain the *user data transferred between the TOE and the terminal connected*.

Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

Asset: confidentiality of logical travel document data

Application note 5: A product using Basic Inspection System with Basic Access Control cannot avert this threat in the context of the security policy defined in this ST.

- **T.Forgery** **Forgery of Data**

Adverse action: An attacker fraudulently alters the *User Data* or/and *TSF-data stored on the travel document* or/and *exchanged between the TOE and the terminal connected* in order to outsmart the PACE authenticated BIS-PACE by means of changed travel document holder's related reference data (like biographic or biometric data). The attacker does it in such a way that the terminal connected perceives these modified data as authentic one.

Threat agent: having high attack potential

Asset: integrity of the travel document

Application note 6: T.Forgery from [PACEPP] is extended here to all kinds of (PACE terminals and EAC2 terminals) targets that are outsmarted by the attacker.

- **T.Information_Leakage** **Information Leakage from travel document**

  Adverse action: An attacker may exploit information leaking from the TOE during its usage in order to disclose confidential *User Data* or/and *TSF-data stored on the travel document* or/and *exchanged between the TOE and the terminal connected*. The information leakage may be inherent in the normal operation or caused by the attacker.

  Threat agent: having high attack potential.

  Asset: confidentiality of User Data and TSF-data of the travel document.

  Application note 7: Leakage may occur through emanations, variations in power consumption, I/O characteristics, clock frequency, or by changes in processing time requirements. This leakage may be interpreted as a covert channel transmission, but is more closely related to measurement of operating parameters which may be derived either from measurements of the contactless interface (emanation) or direct measurements (by contact to the chip still available even for a contactless chip) and can then be related to the specific operation being performed. Examples are Differential Electromagnetic Analysis (DEMA) and Differential Power Analysis (DPA). Moreover the attacker may try actively to enforce information leakage by fault injection (e.g. Differential Fault Analysis).

  Application note 8: Confidential user data in T.Information_Leakage from [PACEPP] include sensitive user data defined in this ST.

- **T.Malfunction** **Malfunction due to Environmental Stress**

  Adverse action: An attacker may cause a malfunction the travel document's hardware and Embedded Software by applying environmental stress in order to (i) deactivate or modify security features or functionality of the TOE' hardware or to (ii) circumvent, deactivate or modify security functions of the TOE's Embedded Software. This may be achieved e.g. by operating the travel document outside the normal operating conditions, exploiting errors in the travel document's Embedded

Software or misusing administrative functions. To exploit these vulnerabilities an attacker needs information about the functional operation.

Threat agent: having high attack potential, being in possession of one or more legitimate travel documents, having information about the functional operation

Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

Application note 9: A malfunction of the TOE may also be caused using a direct interaction with elements on the chip surface. This is considered as being a manipulation (refer to the threat T.Phys-Tamper) assuming a detailed knowledge about TOE's internals.

- **T.Phys-Tamper** **Physical Tampering**

  Adverse action: An attacker may perform physical probing of the travel document in order (i) to disclose the TSF-data, or (ii) to disclose/reconstruct the TOE's Embedded Software. An attacker may physically modify the travel document in order to alter (I) its security functionality (hardware and software part, as well), (ii) the User Data or the TSF-data stored on the travel document.

  Threat agent: having high attack potential, being in possession of one or more legitimate travel documents

  Asset: integrity and authenticity of the travel document, availability of the functionality of the travel document, confidentiality of User Data and TSF-data of the travel document

  Application note 10: Physical tampering may be focused directly on the disclosure or manipulation of the user data (e.g. the biometric reference data for the inspection system) or the TSF data (e.g. authentication key of the travel document) or indirectly by preparation of the TOE to following attack methods by modification of security features (e.g. to enable information leakage through power analysis). Physical tampering requires a direct interaction with the travel document's internals. Techniques commonly employed in IC failure analysis and IC reverse engineering efforts may be used. Before that, hardware security mechanisms and layout characteristics need to be identified. Determination of software design including

treatment of the user data and the TSF data may also be a pre-requisite. The modification may result in the deactivation of a security function. Changes of circuitry or data can be permanent or temporary.

- **T.Skimming** **Skimming travel document / Capturing Card-Terminal Communication**

  Adverse action: An attacker imitates an inspection system in order to get access to the *user data stored on* or *transferred between the TOE and the inspecting authority* connected via the contactless/contact interface of the TOE.

  Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

  Asset: confidentiality of logical travel document data

  Application note 11: A product using BIS-BAC cannot avert this threat in the context of the security policy defined in this ST.

  Application note 12: MRZ is printed and CAN is printed or stuck on the travel document. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted-revealable, cf. OE.Travel_Document_Holder.

- **T.Tracing** **Tracing travel document**

  Adverse action: An attacker tries to gather TOE *tracing data* (i.e. to trace the movement of the travel document) unambiguously identifying it remotely by establishing or listening to a communication via the contactless/contact interface of the TOE.

  Threat agent: having high attack potential, cannot read and does not know the correct value of the shared password (PACE password) in advance.

  Asset: privacy of the travel document holder

  Application note 13: This Threat completely covers and extends “T.Chip-ID” from BAC PP [BACPP].

  Application note 14: A product using BAC (whatever the type of the inspection system is: BIS-BAC) cannot avert this threat in the context of the security policy defined in this ST.

4.2.6. Threats from [SSCDPP]

Threat agents:

1. **Attacker:** Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

The current section also includes all threats of [SSCDPP].

- **T.DTBS_Forgery** **Forgery of the DTBS/R**
  An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

- **T.Hack_Phys** **Physical attacks through the TOE interfaces**
  An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

- **T.SCD_Derive** **Derive the signature-creation data**
  An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

- **T.SCD_Divulg** **Storing, copying, and releasing of the signature-creation data**
  An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature-creation in the TOE.

- **T.Sig_Forgery** **Forgery of the digital signature**
  An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

- **T.SigF_Misuse** **Misuse of the signature-creation function of the TOE**
  An attacker misuses the signature-creation function of the TOE to create a digital signature for data the signatory has not

decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

- **T.SVD_Forgery** **Forgery of the signature-verification data**
  An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

4.3. Organizational Security Policies

The TOE shall comply with the following Organizational Security Policies (OSP) as security rules, procedures, practices, or guidelines imposed by an organization upon its operations (see CC part 1, sec. 3.2).

4.3.1. OSPs from [MR.ED-PP]

The next OSP addresses the need of a policy for the document manufacturer. It is formulated akin to [ICPP].

- **P.Lim_Block_Loader**

  The composite manufacturer uses the Loader for loading of Security IC Embedded Software, user data of the Composite Product or IC Dedicated Support Software in charge of the IC Manufacturer. She limits the capability and blocks the availability of the Loader[5] in order to protect stored data from disclosure and manipulation.

4.3.2. OSPs from [MR.ED-ON-PP]

This section includes the following OSPs from [MR.ED-ON-PP].

- **P.Code_Confidentiality**

  Update code packages that are created by the TOE software developer or document manufacturer are kept confidential, are encrypted after development at the site of the electronic document manufacturer, and are delivered to the TOE in encrypted form.

- **P.Secure_Environment**

  Update terminals are placed in a secure environment that prevents unauthorized physical access, and are operated by authorized staff only. Authorized staff oversees the complete update procedure.

[5] Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.

- **P.Eligible_Terminals_Only**

  Update terminals (i.e. terminals with appropriate certificates that are able to install updates) are handed only to those entities where P.Secure_Environment is enforced. In case of a security incident, these update terminals are functionally disabled (through organizational and/or cryptographic means by e.g. withdrawing certificates).

4.3.3. OSPs from [EAC1PP]

This section includes the following OSPs from [EAC1PP], if the TOE contains EAC1-protected data.

- **P.Personalisation** **Personalisation of the travel document by issuing State or Organisation only**
  The issuing State or Organisation guarantees the correctness of the biographical data, the printed portrait and the digitized portrait, the biometric reference data and other data of the logical travel document with respect to the travel document holder. The personalisation of the travel document for the holder is performed by an agent authorized by the issuing State or Organisation only.

- **P.Sensitive_Data** **Privacy of sensitive biometric reference data**
  The biometric reference data of finger(s) (EF.DG3) and iris image(s) (EF.DG4) are sensitive private personal data of the travel document holder. The sensitive biometric reference data can be used only by inspection systems which are authorized for this access at the time the travel document is presented to the inspection system (Extended Inspection Systems). The issuing State or Organisation authorizes the Document Verifiers of the receiving States to manage the authorization of inspection systems within the limits defined by the Document Verifier Certificate. The travel document's chip shall protect the confidentiality and integrity of the sensitive private personal data even during transmission to the Extended Inspection System after Chip Authentication Version 1.

4.3.4. OSPs from [EAC2PP]

This section includes the following OSPs from [EAC2PP]. They mainly concern EAC2-protected data. As the TOE doesn't support the Restricted Identity Protocol, the P.RestrictedIdentity is not included.

- **P.EAC2_Terminal** **Abilities of Terminals executing EAC Version 2**
  Terminals that intent to be EAC2 terminals must implement the respective terminal part of the protocols required to execute EAC version 2 according to [TR03110-2], and store (static keys) or generate (temporary keys and nonces) the corresponding credentials.

- ~~**P.RestrictedIdentity** **Restricted Identity and Sector's Static Key Pairs**~~
  ~~If the TOE supports the Restricted Identity protocol, the electronic document issuer shall ensure that the Restricted Identity key pair is generated securely and the private keys are stored securely in the electronic document as defined in [TR03110-2].~~

- **P.Terminal_PKI** **PKI for Terminal Authentication**
  The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate available to the personalization agent or the manufacturer.

For the remaining OSPs from [EAC2PP], cf. the next section.

4.3.5. OSPs from [PACEPP]

This PP includes the following OSPs from [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP].

- **P.Card_PKI** **PKI for Passive Authentication (issuing branch)**

  Application note 15: The description below states the responsibilities of involved parties and represents the logical, but not the physical structure of the PKI. Physical distribution ways shall be implemented by the involved parties in such a way that all certificates belonging to the PKI are securely distributed / made available to their final destination, e.g. by using directory services.

  1) The travel document Issuer shall establish a public key infrastructure for the passive authentication, i.e. for digital signature creation and verification for the travel document. For this aim, he runs a Country Signing Certification Authority (CSCA). The travel document Issuer shall publish the CSCA Certificate (CCSCA).

2) The CSCA shall securely generate, store and use the CSCA key pair. The CSCA shall keep the CSCA Private Key secret and issue a self-signed CSCA Certificate (CCSCA) having to be made available to the travel document Issuer by strictly secure means, see [ICAO9303], 5.5.1. The CSCA shall create the Document Signer Certificates for the Document Signer Public Keys (CDS) and make them available to the travel document Issuer, see [ICAO9303], 5.5.1.
3) A Document Signer shall (i) generate the Document Signer Key Pair, (ii) hand over the Document Signer Public Key to the CSCA for certification, (iii) keep the Document Signer Private Key secret and (iv) securely use the Document Signer Private Key for signing the Document Security Objects of travel documents.

- **P.Manufact** **Manufacturing of the travel document's chip**
  The Initialization Data are written by the IC Manufacturer to identify the IC uniquely. The travel document Manufacturer writes the Pre-personalisation Data which contains at least the Personalisation Agent Key.

- **P.Pre-Operational** **Pre-operational handling of the travel document**
  1) The travel document Issuer issues the travel document and approves it using the terminals complying with all applicable laws and regulations.
  2) The travel document Issuer guarantees correctness of the user data (amongst other of those, concerning the travel document holder) and of the TSF-data permanently stored in the TOE[6].
  3) The travel document Issuer uses only such TOE's technical components (IC) which enable traceability of the travel documents in their manufacturing and issuing life cycle phases, i.e. before they are in the operational phase, cf. sec. 1.2.3 of [PACEPP].
  4) If the travel document Issuer authorises a Personalisation Agent to personalise the travel document for travel document holders, the travel document Issuer has to ensure that the Personalisation Agent acts in accordance with the travel document Issuer's policy.

- **P.Terminal** **Abilities and trustworthiness of terminals**

[6] cf. Table 1 and Table 2 of [PACEPP].

The Basic Inspection Systems with PACE (BIS-PACE) shall operate their terminals as follows:

1) The related terminals (basic inspection system) shall be used by terminal operators and by travel document holders as defined in [ICAO9303].
2) They shall implement the terminal parts of the PACE protocol [ICAO9303], of the Passive Authentication [ICAO9303] and use them in this order[7]. The PACE terminal shall use randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).
3) The related terminals need not to use any own credentials.
4) They shall also store the Country Signing Public Key and the Document Signer Public Key (in form of CCSCA and CDS) in order to enable and to perform Passive Authentication (determination of the authenticity of data groups stored in the travel document, [ICAO9303]).
5) The related terminals and their environment shall ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to [PACEPP].

- **P.Trustworthy_PKI** **Trustworthiness of PKI**
  The CSCA shall ensure that it issues its certificates exclusively to the rightful organisations (DS) and DSs shall ensure that they sign exclusively correct Document Security Objects to be stored on the travel document.

4.3.6. OSPs from [SSCDPP]

The current section also includes all OSPs of [SSCDPP].

- **P.CSP_QCert** **Qualified certificate**
  The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (The Directive[DIR][8]: 2:9, Annex I of [DIR]) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole

[7] This order is commensurate with [ICAO9303].

[8] Se mantienen las referencias a [DIR] por respetar los perfiles de protección originales [SSCDPP], [SSCDPP4] y [SSCDPP5], pero estas referencias se deben entender realizadas a [eIDAS] toda vez que en el Anexo de la [DE] se referencian los mismos perfiles de protección [SSCDPP], [SSCDPP4] y [SSCDPP5] para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas según se indica en los informes de mantenimiento [MR2], [MR4] y [MR5].

control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

- **P.QSign** **Qualified electronic signatures**
  The signatory uses a signature-creation system to sign data with an advanced electronic signature (The Directive[DIR]: 1, 2), which is a qualified electronic signature if it is based on a valid qualified certificate (Annex I of [DIR])[9]. The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the digital signature created with a SCD implemented in the SSCD that the signatory maintain under his sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

- **P.Sig_Non-Repud** **Non-repudiation of signatures**

  The life cycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in his un-revoked certificate.

- **P.Sigy_SSCD** **TOE as secure signature-creation device**
  The TOE meets the requirements for an SSCD laid down in Annex III of [DIR]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

4.4. Assumptions

The assumptions describe the security aspects of the environment in which the TOE will be used or is intended to be used. This section includes the assumptions from the claimed protection profiles as listed below and defines no further assumptions.

4.4.1. Assumptions from [EAC1PP]

This section includes the following assumptions from the [EAC1PP]. They concern EAC1-protected data.

- **A.Auth_PKI** **PKI for Inspection Systems**
  The issuing and receiving States or Organisations establish a public key infrastructure for card verifiable certificates of the Extended Access Control. The Country Verifying Certification Authorities, the Document

[9] It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

Verifier and Extended Inspection Systems hold authentication key pairs and certificates for their public keys encoding the access control rights. The Country Verifying Certification Authorities of the issuing States or Organisations are signing the certificates of the Document Verifier and the Document Verifiers are signing the certificates of the Extended Inspection Systems of the receiving States or Organisations. The issuing States or Organisations distribute the public keys of their Country Verifying Certification Authority to their travel document's chip.

Justification:

This assumption only concerns the EAC part of the TOE. The issuing and use of card verifiable certificates of the Extended Access Control is neither relevant for the PACE part of the TOE nor will the security objectives of the [PACEPP] be restricted by this assumption. For the EAC functionality of the TOE the assumption is necessary because it covers the pre-requisite for performing the Terminal Authentication Protocol Version 1.

- **A.Insp_Sys** **Inspection Systems for global interoperability**

  The Extended Inspection System (EIS) for global interoperability (i) includes the Country Signing CA Public Key and (ii) implements the terminal part of PACE [ICAO9303] and/or BAC [BACPP]. BAC may only be used if supported by the TOE. If both PACE and BAC are supported by the TOE and the IS, PACE must be used. The EIS reads the logical travel document under PACE or BAC and performs the Chip Authentication v.1 to verify the logical travel document and establishes secure messaging. EIS supports the Terminal Authentication Protocol v.1 in order to ensure access control and is authorized by the issuing State or Organisation through the Document Verifier of the receiving State to read the sensitive biometric reference data.

  Justification:

  The assumption A.Insp_Sys does not confine the security objectives of the [PACEPP] as it repeats the requirements of P.Terminal and adds only assumptions for the Inspection Systems for handling the the EAC functionality of the TOE.

4.4.2. Assumptions from [EAC2PP]

[EAC2PP] only includes the assumption from [PACEPP] (see below) and defines no other assumption.

4.4.3. Assumptions from [PACEPP]

This section includes the following assumptions from [PACEPP], since both [EAC1PP] and [EAC2PP] claim [PACEPP].

- **A.Passive_Auth** **PKI for Passive Authentication**

  The issuing and receiving States or Organisations establish a public key infrastructure for passive authentication i.e. digital signature creation and verification for the logical travel document. The issuing State or Organisation runs a Certification Authority (CA) which securely generates, stores and uses the Country Signing CA Key pair. The CA keeps the Country Signing CA Private Key secret and is recommended to distribute the Country Signing CA Public Key to ICAO, all receiving States maintaining its integrity. The Document Signer (i) generates the Document Signer Key Pair, (ii) hands over the Document Signer Public Key to the CA for certification, (iii) keeps the Document Signer Private Key secret and (iv) uses securely the Document Signer Private Key for signing the Document Security Objects of the travel documents. The CA creates the Document Signer Certificates for the Document Signer Public Keys that are distributed to the receiving States and Organisations. It is assumed that the Personalisation Agent ensures that the Document Security Object contains only the hash values of genuine user data according to [ICAO9303].

4.4.4. Assumptions from [SSCDPP]

The current section includes all assumptions of [SSCDPP].

- **A.CGA** **Trustworthy certification-generation application**
  The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

- **A.SCA** **Trustworthy signature-creation application**
  The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of the data the signatory wishes to sign in a form appropriate for signing by the TOE.

5. Security Objectives

This chapter describes the security objectives for the TOE and for the TOE environment. The security objectives for the TOE environment are separated into security objectives for the development, and production environment and security objectives for the operational environment.

5.1. Security Objectives for the TOE

5.1.1. Security Objectives for the TOE from [MR.ED-PP]

This section describes the security objectives for the TOE, addressing the aspects of identified threats to be countered by the TOE, and organizational security policies to be met by the TOE.

- **OT.Non_Interfere** **No interference of Access Control Mechanisms**
  The various implemented access control mechanisms must be consistent. Their implementation must not allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

A loader is a part of the chip operating system that allows to load data, i.e. the file-system/applet containing (sensitive) user data, TSF data etc. into the Flash or EEPROM memory after delivery of the smartcard to the document manufacturer.

The following objective for the TOE addresses limiting the availability of the loader, and is formulated akin to [ICPP].

- **OT.Cap_Avail_Loader** **Capability and availability of the Loader**
  The TSF provides limited capability of the Loader functionality of the TOE embedded software and irreversible termination of the Loader in order to protect user data from disclosure and manipulation.

5.1.2. Security Objectives for the TOE from [MR.ED-ON-PP]

This section includes the following additional security objectives for the TOE from [MR.ED-ON-PP].

- **OT.Update_Mechanism** **TOE Update Mechanism**

  The TSF provides a mechanism to install code-signed updates of the TOE software by authorized staff during operational use.

- **OT.Enc_Sign_Update** **Encrypted-then-signed Update Packages**

  The TOE only installs update packages that are encrypted, integrity-protected and signed by the authority in charge of delivering and installing updates.

- **OT.Update_Terminal_Auth** **Updates only by authenticated Update Terminals**

  The TOE allows only authenticated update terminals to upload an update package to the TOE and to initiate the update procedure. The TOE uses a dedicated cryptographic method described in [GOA] to authenticate an update terminal.

- **OT.Attack_Detection Mechanism** **Detection of Attacks on the TOE using the Update**

  The TOE has logging capabilities that track installed updates and failed update attempts. It also limits the amount of faulty (signature verification or decryption fails) update attempts. It allows dedicated terminals to read out the update logs.

- **OT.Key_Secrecy** **Key Secrecy of Cryptographic Update Keys**

  The TOE keeps the cryptographic update keys secret, and is designed such that emissions from the TOE do not allow to read out or gain full or partial information about the keys.

5.1.3. Security Objectives for the TOE from [EAC1PP]

This section includes the following additional security objectives for the TOE from [EAC1PP] that are not included in [PACEPP]. They concern EAC1-protected data.

- **OT.Chip_Auth_Proof** **Proof of the travel document's chip authenticity**

  The TOE must support the Inspection Systems to verify the identity and authenticity of the travel document's chip as issued by the identified issuing State or Organisation by means of the Chip Authentication Version 1 as defined in [TR03110]. The authenticity proof provided by travel document's chip shall be protected against attacks with high attack potential.

  Application note 16: The OT.Chip_Auth_Proof implies the travel document's chip to have (i) a unique identity as given by

the travel document's Document Number, (ii) a secret to prove its identity by knowledge i.e. a private authentication key as TSF data. The TOE shall protect this TSF data to prevent their misuse. The terminal shall have the reference data to verify the authentication attempt of travel document's chip i.e. a certificate for the Chip Authentication Public Key that matches the Chip Authentication Private Key of the travel document's chip. This certificate is provided by (i) the Chip Authentication Public Key (EF.DG14) in the LDS defined in [ICAO9303] and (ii) the hash value of DG14 in the Document Security Object signed by the Document Signer.

- **OT.Sens_Data_Conf** **Confidentiality of sensitive biometric reference data**
  The TOE must ensure the confidentiality of the sensitive biometric reference data (EF.DG3 and EF.DG4) by granting read access only to authorized Extended Inspection Systems. The authorization of the inspection system is drawn from the Inspection System Certificate used for the successful authentication and shall be a non-strict subset of the authorization defined in the Document Verifier Certificate in the certificate chain to the Country Verifier Certification Authority of the issuing State or Organisation. The TOE must ensure the confidentiality of the logical travel document data during their transmission to the Extended Inspection System. The confidentiality of the sensitive biometric reference data shall be protected against attacks with high attack potential.

5.1.4. Security Objectives for the TOE from [EAC2PP]

This section includes the following additional security objectives for the TOE from [EAC2PP] that are not included in [PACEPP]. They concern EAC2-protected data. As the TOE doesn't support the Restricted Identity Protocol, the OT.RI_EAC2 is not included.

- **OT.AC_Pers_EAC2** **Personalization of the Electronic Document**
  The TOE must ensure that user data and TSF-Data that are permanently stored in the TOE can be written by authorized personalization agents only, with the following exception: An EAC2 terminal may also write or modify user data according to its effective access rights. The access rights are determined by the electronic document during Terminal Authentication 2.
  Justification: This security objective for the TOE modifies OT.AC_Pers from [PACEPP] as the additional features of EAC2 allow a strongly controlled, secure and fine-grained access to individual data groups of the electronic document.

- **OT.CA2** **Proof of the Electronic Document's Chip Authenticity**
  The TOE must allow EAC2 terminals to verify the identity and authenticity of the electronic document's chip as being issued by the identified issuing state or organization by Chip Authentication 2 [TR03110-2]. The authenticity of the chip and its proof mechanism provided by the electronic document's chip shall be protected against attacks with high attack potential.

- ~~**OT.RI_EAC2** **Support of Restricted Identity by the TOE**~~
  ~~If the TOE supports pseudonymous authentication, it must use the Restricted Identity protocol as defined in [TR03110-2].~~

- **OT.Sens_Data_EAC2** **Confidentiality of sensitive User Data**
  The TOE must ensure confidentiality of sensitive user data by granting access to sensitive data only to EAC2 terminals with corresponding access rights. The authorization of an EAC2 terminal is the minimum set of the access rights drawn from the terminal certificate used for successful authentication and the corresponding DV and CVCA certificates, and the access rights sent to the electronic document as part of PACE.
  The TOE must ensure confidentiality of all user data during transmission to an EAC2 terminal after Chip Authentication 2. Confidentiality of sensitive user data shall be protected against attacks with high attack potential.

5.1.5. Security Objectives for the TOE from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP]. Therefore the following security objectives are included as well. We list them only once here.

- **OT.AC_Pers** **Access Control for Personalisation of logical MRTD**

  The TOE must ensure that the logical travel document data in EF.DG1 to EF.DG16, the Document Security Object according to LDS [ICAO9303] and the TSF data can be written by authorized Personalisation Agents only. The logical travel document data in EF.DG1 to EF.DG16 and the TSF data may be written only during and cannot be changed after personalisation of the document.

Application note 17: The OT.AC_Pers implies that the data of the LDS groups written during personalisation for travel document holder (at least EF.DG1 and EF.DG2) can not be changed using write access after personalisation.

- **OT.Data_Authenticity** **Authenticity of Data**
  The TOE must ensure authenticity of the User Data and the TSF-data[10] stored on it by enabling verification of their authenticity at the terminal-side[11]. The TOE must ensure authenticity of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication. It shall happen by enabling such a verification at the terminal-side (at receiving by the terminal) and by an active verification by the TOE itself (at receiving by the TOE)[12].

Application note 18: OT.Data_Authenticity from [PACEPP] shall be extended to all kinds of PACE terminals and EAC2 terminals.

- **OT.Data_Confidentiality** **Confidentiality of Data**
  The TOE must ensure confidentiality of the User Data and the TSF-data[13] by granting read access only to the PACE authenticated BIS-PACE connected.The TOE must ensure confidentiality of the User Data and the TSF-data during their exchange between the TOE and the terminal connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

- **OT.Data_Integrity** **Integrity of Data**
  The TOE must ensure integrity of the User Data and the TSF-data[14] stored on it by protecting these data against unauthorised modification (physical manipulation and unauthorised modifying). The TOE must ensure integrity of the User Data and the TSF-data during their exchange between the TOE and the terminal

[10] where appropriate, see Table 2 of [PACEPP]
[11] verification of SO_D
[12] secure messaging after the PACE authentication, see also [ICAO9303]
[13] where appropriate, see Table 2 of [PACEPP]
[14] where appropriate, see Table 2 of [PACEPP]

connected (and represented by PACE authenticated BIS-PACE) after the PACE Authentication.

Application note 19: OT.Data_Integrity from [PACEPP] is extended here to all kinds of PACE terminals and EAC2 terminals. Justification: Obviously, data integrity must be ensured w.r.t. all possible terminal types.

- **OT.Identification** — **Identification of the TOE**
  The TOE must provide means to store Initialisation[15] and Pre-Personalisation Data in its non-volatile memory. The Initialisation Data must provide a unique identification of the IC during the manufacturing and the card issuing life cycle phases of the travel document. The storage of the Pre-Personalisation data includes writing of the Personalisation Agent Key(s).

- **OT.Prot_Abuse-Func** — **Protection against Abuse of Functionality**
  The TOE must prevent that functions of the TOE, which may not be used in TOE operational phase, can be abused in order (i) to manipulate or to disclose the User Data stored in the TOE, (ii) to manipulate or to disclose the TSF-data stored in the TOE, (iii) to manipulate (bypass, deactivate or modify) soft-coded security functionality of the TOE.

- **OT.Prot_Inf_Leak** — **Protection against Information Leakage**
  The TOE must provide protection against disclosure of confidential User Data or/and TSF-data stored and/or processed by the travel document
  - by measurement and analysis of the shape and amplitude of signals or the time between events found by measuring signals on the electromagnetic field, power consumption, clock, or I/O lines,
  - by forcing a malfunction of the TOE and/or
  - by a physical manipulation of the TOE.

  Application note 20: This objective pertains to measurements with subsequent complex signal processing due to normal operation of the TOE or operations enforced by an attacker.

- **OT.Prot_Malfunction** — **Protection against Malfunctions**

[15] amongst other, IC Identification data

The TOE must ensure its correct operation. The TOE must prevent its operation outside the normal operating conditions where reliability and secure operation have not been proven or tested. This is to prevent functional errors in the TOE. The environmental conditions may include external energy (esp. electromagnetic) fields, voltage (on any contacts), clock frequency or temperature.
The following TOE security objectives address the aspects of identified threats to be countered *involving TOE's environment*.

- **OT.Prot_Phys-Tamper** **Protection against Physical Tampering**
The TOE must provide protection of confidentiality and integrity of the User Data, the TSF-data and the travel document's Embedded Software by means of
  - measuring through galvanic contacts representing a direct physical probing on the chip's surface except on pads being bonded (using standard tools for measuring voltage and current) or
  - measuring not using galvanic contacts, but other types of physical interaction between electrical charges (using tools used in solid-state physics research and IC failure analysis),
  - manipulation of the hardware and its security functionality, as well as
  - controlled manipulation of memory contents (User Data, TSF-data)

  with a prior

  - reverse-engineering to understand the design and its properties and functionality.

- **OT.Tracing** **Tracing travel document**
The TOE must prevent gathering TOE tracing data by means of unambiguous identifying the travel document remotely through establishing or listening to a communication via the contactless/contact interface of the TOE without knowledge of the correct values of shared passwords (PACE passwords) in advance.

Application note 21: Since the Standard Inspection Procedure does not support any unique-secret-based authentication of the travel document's chip (no Chip Authentication), a security objective like OT.Chip_Auth_Proof (proof of travel document authenticity)[16] cannot be achieved by the current TOE.

5.1.6. Security objectives for the TOE from [SSCDPP], [SSCDPP4] and [SSCDPP5]

The current section includes all security objectives for the TOE of [SSCDPP], [SSCDPP4] and [SSCDPP5].

- **OT.DTBS_Integrity_TOE** — **DTBS/R integrity inside the TOE**
  The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation..

- **OT.EMSEC_Design** — **Provide physical-emanation security**
  Design and build the TOE in such a way as to control the production of intelligible emanations within specified limits.

- **OT.Lifecycle_Security** — **Lifecycle security**
  The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall provide functionality to securely destroy the SCD on demand of the signatory.

Application note 22: The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

- **OT.SCD_Secrecy** — **Secrecy of the signature-creation data**
  The secrecy of an SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

[16] Such a security objective might be formulated like: 'The TOE must enable the terminal connected to verify the authenticity of the travel document as a whole device as issued by the travel document Issuer (issuing PKI branch of the travel document Issuer) by means of the Passive and Chip Authentication as defined in [ICAO9303]'.

Application note 23: The TOE shall keep the confidentiality of the SCD at all times in particular during SCD/SVD generation, SCD signing operation, storage and by destruction.

- **OT.SCD_SVD_Corresp** **Correspondence between SVD and SCD**
  The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating a digital signature creation with the SCD.

- **OT.SCD_Unique** **Uniqueness of the signature-creation data**
  The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation can practically occur only once and cannot be reconstructed from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

- **OT.SCD/SVD_Auth_Gen** **SCD/SVD authorized generation**
  The TOE provides security features to ensure that authorised users only invoke the generation of the SCD and the SVD.

- **OT.Sig_Secure** **Cryptographic security of the electronic signature**
  The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

- **OT.Sigy_SigF** **Signature creation function for the legitimate signatory only**
  The TOE provides the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others to create a digital signature. The TOE shall resist attacks with high attack potential.

- **OT.Tamper_ID** **Tamper detection**

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

- **OT.Tamper_Resistance** **Tamper resistance**
  The TOE prevents or resists physical tampering with specified system devices and components.

- **OT.TOE_TC_VAD_Imp** **Trusted channel of TOE for VAD import**
  The TOE shall provide a trusted channel for the protection of the confidentiality and integrity of the VAD received from the HID as needed by the authentication method employed.

Application note 24: This security objective for the TOE is partly covering OE.HID_VAD from [SSCDPP]. While OE.HID_VAD in [SSCDPP] requires only the operational environment to protect VAD, [SSCDPP5] requires the HID and the TOE to implement a trusted channel for the protection of the VAD: the HID exports the VAD and establishes one end of the trusted channel according to OE.HID_TC_VAD_Exp, the TOE imports VAD at the other end of the trusted channel according to OT.TOE_TC_VAD_Imp. Therefore [SSCDPP5] re-assigns partly the VAD protection from the operational environment as described by OE.HID_VAD to the TOE as described by OT.TOE_TC_VAD_Imp and leaves only the necessary functionality by the HID.

- **OT.TOE_TC_DTBS_Imp** **Trusted channel of TOE for DTBS import**
  The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

- **OT.TOE_SSCD_Auth** **Authentication proof as SSCD**
  The TOE shall hold unique identity and authentication data as SSCD and provide security mechanisms to identify and to authenticate itself as SSCD.

- **OT.TOE_TC_SVD_Exp** **TOE trusted channel for SVD export**
  The TOE shall provide a trusted channel to the CGA to protect the integrity of the SVD exported to the CGA. The TOE shall enable the CGA to detect alteration of the SVD exported by the TOE.

Note that all are formally included here, but careful analysis reveals that OT.SCD_Secrecy, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, and OT.Tamper_Resistance are actually fully or partly covered by security objectives included from [PACEPP].

5.2. Security Objectives for the Operational Environment

5.2.1. Security objectives from [MR.ED-PP]

The following objective on the environment is defined akin to the objective from [ICPP].

- **OE.Lim_Block_Loader** **Limitation of capability and blocking the Loader**

  The manufacturer will protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly[17] the Loader after intended usage of the Loader.

Justification: This security objective directly addresses the threat **T.Non_Interfere**. This threat concerns the potential interference of different access control mechanisms, which could occur as a result of combining different applications on a smartcard. Such combination does not occur in one of the claimed PPs. Hence, this security objective for the environment does

- neither mitigate a threat of one of the claimed PPs that was addressed by security objectives of that PP,
- nor does it fulfill any organizational security policy of one of the claimed PPs that was meant to be addressed by security objectives of the TOE of that PP.

5.2.2. Security objectives from [MR.ED-ON-PP]

- **OE.Code_Confidentiality**

  The operational environment must ensure that the TOE software developer or document manufacturer keeps update code packages confidential, encrypts them after development at the site of the developer/manufacturer, and delivers them to the TOE in encrypted form.

- **OE.Secure_Environment**

  The operational environment must ensure that update terminals are placed in a secure environment that

[17] Note that blocking the Loader is not required, as only authorized users can use the Loader as stated in BSI.P.Ctrl-Loader.

prevents unauthorized physical access, and are operated by authorized staff only. The operational environment must also ensure through e.g. organizational policies and procedures, that authorized staff oversees the complete update procedure.

- **OE.Eligible_Terminals_Only**

  The operational environment must also ensure by e.g. organizational procedures, supported by cryptographic means, that only those entities that have policies in place that guarantee OE.Secure_Environment, are supplied with update terminals. Moreover the operational environment guarantees that update terminals can be functionally deactivated if these policies are no longer in place or not enforced at the entities. This can be implemented for example by the issuance of certificates for update terminals together with a public key infrastructure.

Justification: Each of these security objectives on the environment directly addresses one of the organizational security policies P.Code_Confidentiality, P.Secure_Environment, and P.Eligible_Terminals_Only. Hence, these security objectives for the environment do

- neither mitigate a threat of the [MR.ED-PP] that was addressed by security objectives of the [MR.ED-PP],
- nor do they fulfill any organizational security policy of the [MR.ED-PP] that was meant to be addressed by security objectives of the TOE of the [MR.ED-PP].

Note in particular that OE.Eligible_Terminals_Only requires a general issuance and revocation mechanism for update terminals and leaves the specific implementation open, whereas OE.Terminal_Authentication of the [MR.ED-PP] specifically addresses certificates for EAC2 terminals.

5.2.3. Security objectives from [EAC1PP]

This section includes the following security objectives for the TOE from the [EAC1PP]. They mainly concern EAC1-protected data.

Issuing State or Organisation

The issuing State or Organisation will implement the following security objectives of the TOE environment.

- **OE.Auth_Key_Travel_Document** **Travel document Authentication Key**
  The issuing State or Organisation has to establish the necessary public key infrastructure in order to (i) generate the travel document's Chip Authentication Key Pair, (ii) sign and store the Chip Authentication Public Key in the Chip Authentication Public Key data in EF.DG14 and (iii) support inspection systems of receiving States or Organisations to verify the authenticity of the travel document's chip used for genuine travel document by certification of the Chip Authentication Public Key by means of the Document Security Object.
  Justification: This security objective for the operational environment is needed additionally to those from [PACEPP] in order to counter the Threat T.Counterfeit as it specifies the pre-requisite for the Chip Authentication Protocol Version 1 which is one of the additional features of the TOE described only in this Security Target and not in [PACEPP].

- **OE.Authoriz_Sens_Data** **Authorization for Use of Sensitive Biometric Reference Data**
  The issuing State or Organisation has to establish the necessary public key infrastructure in order to limit the access to sensitive biometric reference data of travel document holders to authorized receiving States or Organisations. The Country Verifying Certification Authority of the issuing State or Organisation generates card verifiable Document Verifier Certificates for the authorized Document Verifier only.
  Justification: This security objective for the operational environment is needed additionally to those from [PACEPP] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the

need of an PKI for this protocol and the responsibilities of its root instance. The Terminal Authentication Protocol v.1 is one of the additional features of the TOE described only in this Security Target and not in [PACEPP].

Receiving State or Organisation

The receiving State or Organisation will implement the following security objectives of the TOE environment.

- **OE.Exam_Travel_Document** **Examination of the physical part of the travel document**
  The inspection system of the receiving State or Organisation must examine the travel document presented by the traveller to verify its authenticity by means of the physical security measures and to detect any manipulation of the physical part of the travel document. The Basic Inspection System for global interoperability (i) includes the Country Signing CA Public Key and the Document Signer Public Key of each issuing State or Organisation, and (ii) implements the terminal part of PACE [ICAO9303] and/or the Basic Access Control [ICAO9303]. Extended Inspection Systems perform additionally to these points the Chip Authentication Protocol Version 1 to verify the Authenticity of the presented travel document's chip.
  Justification: This security objective for the operational environment is needed additionally to those from [PACEPP] in order to handle the Threat T.Counterfeit and the Assumption A.Insp_Sys by demanding the Inspection System to perform the Chip Authentication protocol v.1. OE.Exam_Travel_Document also repeats partly the requirements from OE.Terminal in [PACEPP] and therefore also counters T.Forgery and A.Passive_Auth from [PACEPP]. This is done because a new type of Inspection System is introduced in this ST as the Extended Inspection System is needed to

handle the additional features of a travel document with Extended Access Control.

- **OE.Ext_Insp_Systems** — **Authorization of Extended Inspection Systems**
  The Document Verifier of receiving States or Organisations authorizes Extended Inspection Systems by creation of Inspection System Certificates for access to sensitive biometric reference data of the logical travel document. The Extended Inspection System authenticates themselves to the travel document's chip for access to the sensitive biometric reference data with its private Terminal Authentication Key and its Inspection System Certificate.
  Justification: This security objective for the operational environment is needed additionally to those from [PACEPP] in order to handle the Threat T.Read_Sensitive_Data, the Organisational Security Policy P.Sensitive_Data and the Assumption A.Auth_PKI as it specifies the pre-requisite for the Terminal Authentication Protocol v.1 as it concerns the responsibilities of the Document Verifier instance and the Inspection Systems.

- **OE.Prot_Logical_Travel_Document** — **Protection of data from the logical travel document**
  The inspection system of the receiving State or Organisation ensures the confidentiality and integrity of the data read from the logical travel document. The inspection system will prevent eavesdropping to their communication with the TOE before secure messaging is successfully established based on the Chip Authentication Protocol Version 1.
  Justification: This security objective for the operational environment is needed additionally to those from [PACEPP] in order to handle the Assumption A.Insp_Sys by requiring the Inspection System to perform secure messaging based on the Chip Authentication Protocol v.1.

5.2.4. Security Objectives from [EAC2PP]

This PP includes the following security objectives for the TOE from the [EAC2PP]. They mainly concern EAC2-protected data. As the TOE doesn't support the Restricted Identity Protocol, the OE.RestrictedIdentity is not included.

- **OE.Chip_Auth_Key** **Key Pair needed for Chip Authentication**
  The electronic document issuer has to ensure that the electronic document's chip authentication key pair is generated securely, that the private keys of this key pair is stored correctly in the electronic document's chip, and that the corresponding public keys are distributed to the EAC2 terminals that are used according to [TR03110-2] to check the authenticity of the electronic document's chip.
  Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of an electronic document (i.e. protection against cloning). Therefore, this *additional* security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

- ~~**OE.RestrictedIdentity** **Restricted Identity and Sector's Static Key Pairs**~~
  ~~If the TOE supports pseudonymous identification and thus implements the Restricted Identity protocol, the electronic document issuer has to ensure that the Restricted Identity key pair is generated securely and the private keys are stored securely in the electronic document as required according to [TR03110-2].~~
  ~~**Justification:** The TSF of [PACEPP] does not include any mechanism to identify the document holder by using a pseudonym. Therefore, this *additional* security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].~~

- **OE.Terminal_Authentication** **Key pairs needed for Terminal Authentication**
  The electronic document issuer shall establish a public key infrastructure for the card verifiable certificates used for Terminal Authentication. For this aim, the electronic document issuer shall run a Country Verifying Certification Authority. The instances of the PKI shall fulfill the requirements and rules of the corresponding certificate policy. The electronic document issuer shall make the CVCA certificate

available to the personalization agent or the manufacturer.

Justification: The TSF of [PACEPP] does not include any mechanism to verify the authenticity of the terminal that reads out the data stored on the electronic document (by successfully executing PACE, a terminal only proves knowledge of the PACE password). Therefore, this *additional* security objective for the operational environment does not mitigate any threat of, and does not fulfill any OSP of [PACEPP].

For the remaining ones, see the next section.

5.2.5. Security Objectives from [PACEPP]

Both [EAC1PP] and [EAC2PP] claim [PACEPP]. Therefore the following security objectives on the operational environment are included as well.

Travel document Issuer as the general responsible

The travel document Issuer as the general responsible for the global security policy related will implement the following security objectives for the TOE environment:

- **OE.Legislative_Compliance** **Issuing of the travel document**
  The travel document Issuer must issue the travel document and approve it using the terminals complying with all applicable laws and regulations.

Travel document Issuer and CSCA: travel document's PKI (issuing) branch

The travel document Issuer and the related CSCA will implement the following security objectives for the TOE environment (see also the Application note 15 above):

- **OE.Passive_Auth_Sign** **Authentication of travel document by Signature**
  The travel document Issuer has to establish the necessary public key infrastructure as follows: the CSCA acting on behalf and according to the policy of the travel document Issuer must (i) generate a cryptographically secure CSCA Key Pair, (ii) ensure the secrecy of the CSCA Private Key and sign Document Signer Certificates in a secure operational environment, and (iii) publish the Certificate of the CSCA Public Key (C_{CSCA}). Hereby authenticity and integrity of these certificates are being maintained. A Document Signer acting in accordance with the CSCA policy must (i) generate a cryptographically secure

Document Signing Key Pair, (ii) ensure the secrecy of the Document Signer Private Key, (iii) hand over the Document Signer Public Key to the CSCA for certification, (iv) sign Document Security Objects of genuine travel documents in a secure operational environment only. The digital signature in the Document Security Object relates to all hash values for each data group in use according to [ICAO9303]. The Personalisation Agent has to ensure that the Document Security Object contains only the hash values of genuine user data according to [ICAO9303]. The CSCA must issue its certificates exclusively to the rightful organisations (DS) and DS_S must sign exclusively correct Document Security Objects to be stored on travel document.

- **OE.Personalisation** — **Personalisation of travel document**
  The travel document Issuer must ensure that the Personalisation Agents acting on his behalf (i) establish the correct identity of the travel document holder and create the biographical data for the travel document, (ii) enrol the biometric reference data of the travel document holder, (iii) write a subset of these data on the physical Passport (optical personalisation) and store them in the travel document (electronic personalisation) for the travel document holder as defined in [ICAO9303][18], (iv) write the document details data, (v) write the initial TSF data, (vi) sign the Document Security Object defined in [ICAO9303] (in the role of a DS).

Terminal operator: Terminal's receiving branch

- **OE.Terminal** — **Terminal operating**
  The terminal operators must operate their terminals as follows:
  1) The related terminals (basic inspection systems) are used by terminal operators and by travel document holders as defined in [ICAO9303].
  2) The related terminals implement the terminal parts of the PACE protocol [ICAO9303], of the Passive Authentication [ICAO9303] (by verification of the signature of the

[18] see also [ICAO9303], part 11

Document Security Object) and use them in this order[19]. The PACE terminal uses randomly and (almost) uniformly selected nonces, if required by the protocols (for generating ephemeral keys for Diffie-Hellmann).

3) The related terminals need not to use any own credentials.
4) The related terminals securely store the Country Signing Public Key and the Document Signer Public Key (in form of C_{CSCA} and C_{DS}) in order to enable and to perform Passive Authentication of the travel document (determination of the authenticity of data groups stored in the travel document, [ICAO9303]).
5) The related terminals and their environment must ensure confidentiality and integrity of respective data handled by them (e.g. confidentiality of the PACE passwords, integrity of PKI certificates, etc.), where it is necessary for a secure operation of the TOE according to the current ST.

Application note 25: OE.Terminal completely covers and extends "OE.Exam_MRTD", "OE.Passive_Auth_Verif" and "OE.Prot_Logical_MRTD" from BAC PP [BACPP].

Application note 26: Opposite to OE.Terminal from [PACEPP], a terminal supporting EAC2 according to [TR03110-2] needs to store its own credentials for Extended Access Control.

Travel document holder Obligations

- **OE.Travel_Document_Holder** **Travel document holder Obligations**
  The travel document holder may reveal, if necessary, his or her verification values of the PACE password to an authorized person or device who definitely act according to respective regulations and are trustworthy.

5.2.6. Security Objectives from [SSCDPP], [SSCDPP4] y [SSCDPP5]

This section includes all security objectives for the TOE of [SSCDPP], [SSCDPP4] y [SSCDPP5].

- **OE.CGA_QCert** **Generation of qualified certificates**
  The CGA shall generate a qualified certificate that includes (amongst others)
  - the name of the signatory controlling the TOE,
  - the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
  - the advanced signature of the CSP.

[19] This order is commensurate with [ICAO9303].

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

- **OE.DTBS_Intend** **SCA sends data intended to be signed**
  The Signatory uses trustworthy SCA that
  - generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
  - sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
  - attaches the signature produced by the TOE to the data or provides it separately.

  - Application note 27*: The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.*
  -

- **OE.SCA_TC_DTBS_Exp**[20] **Trusted channel of SCA for DTBS export.**
  The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

- **OE.HID_TC_VAD_Exp**[21] **Trusted channel of HID for VAD export.**

[20] Dado que el TOE incluye la funcionalidad del canal seguro, este OE es el resultado de adaptar el OE.DTBS_Protect de [SSCDPP] tal y como se indica en [SSCDPP5].
[21] Dado que el TOE incluye la funcionalidad del canal seguro, este OE es el resultado de adaptar el OE.HI_VAD de [SSCDPP] tal y como se indica en [SSCDPP5].

The HID provides the human interface for user authentication. The HID will ensure confidentiality and integrity of the VAD as needed by the authentication method employed including export to the TOE by means of a trusted channel.

- **OE.Signatory** — **Security obligation of the Signatory**
  The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

- **OE.SVD_Auth** — **Authenticity of the SVD**
  The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

- **OE.Dev_Prov_Service** — **Authentic SSCD provided by SSCD Provisioning Service**
  The SSCD Provisioning Service handles authentic devices that implement the TOE, prepares the TOE for proof as SSCD to external entities, personalises the TOE for the legitimate user as signatory, links the identity of the TOE as SSCD with the identity of the legitimate user, and delivers the TOE to the signatory.

  Note: This objective replaces OE.SSCD_Prov_Service from the [SSCDPP], which is possible as it does not imply any additional requirements for the operational environment when compared to OE.SSCD_Prov_Service (OE.Dev_Prov_Service is a subset of OE.SSCD_Prov_Service).

- **OE.CGA_SSCD_Auth** — **Pre-initialisation of the TOE for SSCD authentication**
  The CSP shall check by means of the CGA whether the device presented for application of a (qualified) certificate holds unique identification as SSCD, successfully proved this identity as SSCD to the CGA, and whether this identity is linked to the legitimate holder of the device as applicant for the certificate.

- **OE.CGA_TC_SVD_Imp** — **CGA trusted channel for SVD import**
  The CGA shall detect alteration of the SVD imported from the TOE with the claimed identity of the SSCD.

The developer prepares the TOE by pre-initialisation for the delivery to the customer (i.e. the SSCD provisioning service) in the development phase not addressed by a security objective for the operational environment. The SSCD Provisioning Service performs initialisation and personalisation as TOE for the legitimate user (i.e. the Device holder). If the TOE is delivered to the Device holder with SCD the TOE is a SSCD. This situation is addressed by OE.SSCD_Prov_Service except the additional initialisation of the TOE for proof as SSCD and trusted channel to the CGA. If the TOE is delivered to the Device holder without a SCD the TOE will be a SSCD only after generation of the first SCD/SVD pair. Because this SCD/SVD pair generation is performed by the signatory in the operational use stage the TOE provides additional security functionality addressed by OT.TOE_SSCD_Auth and OT.TOE_TC_SVD_Exp. But this security functionality must be initialised by the SSCD Provisioning Service as described in OE.Dev_Prov_Service. Therefore this ST substitutes OE.SSCD_Prov_Service by OE.Dev_Prov_Service allowing generation of the first SCD/SVD pair after delivery of the TOE to the Device holder and requiring initialisation of security functionality of the TOE. Nevertheless the additional security functionality must be used by the operational environment as described in OE.CGA_SSCD_Auth and OE.CGA_TC_SVD_Imp. This approach does not weaken the security objectives of and requirements to the TOE but enforce more security functionality of the TOE for additional method of use. Therefore it does not conflict with the CC conformance claim to the [SSCDPP].

5.3. Security Objective Rationale

Tabla 2 provides an overview of the security objectives' coverage. According to CC part 1 [CC], the tracing between security objectives and the security problem definition must ensure that 1) *each security objective traces to at least one threat, OSP and assumption*, 2) *each threat, OSP and assumption has at least one security objective tracing to it*, and 3) *the tracing is correct* (i.e. the main point being that security objectives for the TOE do not trace back to assumptions).

This is illustrated in the following way:

1) Security objectives from claimed PPs are traced to their corresponding thread, OSP and assumption in respective claimed PP security objective rationale section.
2) Newly introduced security objectives (i.e. **OE.Lim_Block_Loader** and **OT.Cap_Avail_Loader**) are traced to their corresponding thread, OSP and assumption by checking the *columns* of **Tabla 2**.
3) Threads, OSPs and assumptions from claimed PPs have at least one security objective tracing to it in respective claimed PP security objective rationale section.
4) Newly introduced threads, OSPs and assumptions (i.e **P.Lim_Block_Loader** and **T.InconsistentSec**) have at least one security objective from claimed PPs or newly introduced security objective tracing to it by checking *rows* of **Tabla 2.**
5) Simply by checking the *columns* of **Tabla 2** and the security objective rationales from the claimed PPs.

	OT.AC_Pers	OT.AC_Pers_EAC2	OT.Cap_Avail_Loader	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Non_Interfere	OT.Sens_Data_Conf (EAC1PP)	OT.Sens_Data_EAC2	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OE.Lim_Block_Loader	OE.Code_Confidentiality	OE.Secure_Environment	OE.Eligible_Terminals_Only
T.InconsistentSec	X	X	X	X	X	X	X	X	X						X			
T.Interfere							X											
T.FaTSF										X			X	X				
T.UaU											X	X						
P.Lim_Block_Loader			X				X								X			
P.Code_Confidentiality																X		
P.Secure_Environment																	X	
P.Eligible_Terminals_Only																		X

Tabla 2.- Security Objective Rationale

The threat **T.InconsistentSec** addresses attacks on the confidentiality and the integrity of user data stored on the TOE, facilitated by the data not being protected as intended.

OT.AC_Pers and OT.AC_Pers_EAC2 define the restriction on writing or modifying data;

OT.Data_Authenticity, OT.Data_Confidentiality, OT.Data_Integrity, OT.Sens_Data_Conf (from [EAC1PP]), and OT.Sens_Data_EAC2 require the security of stored user data as well as user data that are transferred between the TOE and a terminal to be secure w.r.t. authenticity, integrity and confidentiality.

OT.Non_Interfere requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

OT.Cap_Avail_Loader requires the TOE to provide limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data.

OE.Lim_Block_Loader requires the manufacturer to protect the loader functionality against misuse, limit the capability of the loader, and terminate irreversibly the loader after intended usage of the loader.

The combination of these security objectives cover the threat posed by **T.InconsistentSec**.

The threat **T.Interfere** addresses the attack on user data by exploiting the unintended interference of security protocols. This is directly countered by OT.Non_Interfere, requiring the

TOE's access control mechanisms to be implemented consistently, and their implementations to not allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one.

The threat **T.FaTSF** addresses attacks on the TOE and TSF by an attacker exploiting flaws of the TOE software implementation that manifest themselves after the TOE enters the phase operational usage. This threat is countered by the TOE offering a secure update mechanism; in particular:

- The security objective OT.Update_Mechanism counters this threat by ensuring that the TOE has the ability to update the TOE software in a secure manner.
- The security objective OT.Attack_Detection ensures that the TOE is able to detect multiple failed update attempts and can take action upon that detection.
- The security objective OT.Key_Secrecy makes sure that the required cryptographic key material for the update mechanism cannot be accessed or reconstructed by a malicious attacker.

The threat **T.UaU** addresses attacks on the TOE and TSF by an attacker installing unauthorized and potential harmful updates:

- The security objective OT.Enc_Sign_Update ensures that only signed and encrypted updates are installed by the TOE, and that during the transmission to the TOE, a protocol based on encrypt-then-MAC is used.
- The security objective OT.Update_Terminal_Auth ensures that only authenticated update terminals are able to update version information, upload update packages on the TOE, and initiate the update procedure.

The OSP **P.Lim_Block_Loader** addresses limiting the capability and blocking the availability of the Loader in order to protect stored data from disclosure and manipulation. This is addressed by OT.Cap_Avail_Loader, which requires the TOE to provide a limited capability of the loader functionality and irreversible termination of the loader in order to protect stored user data; by OT.Non_Interfere, which requires the TOE's access control mechanisms to be implemented consistently and their implementations not to allow to circumvent an access control mechanism by exploiting an unintended implementational interference of one access control mechanism with another one; and by OE.Lim_Block_Loader, which requires the manufacturer to protect the Loader functionality against misuse, limit the capability of the Loader and terminate irreversibly the Loader after intended usage of the Loader.

The organizational security policies **P.Code_Confidentiality**, **P.Secure_Environment**, and **P.Eligible_Terminals_Only**, address the confidentiality of the code, the way the update procedure must be carried out, and precise control over which terminals are allowed to carry out the update procedure. Each of these policies are enforced through security objectives for the environment of the TOE, namely OE.Code_Confidentiality, OE.Secure_Environment, and OE.Eligible_Terminals_Only.

6. Extended Components Definition

This section includes all extended components from the claimed PPs. This includes

- FAU_SAS.1 from the family FAU_SAS from [PACEPP]

To describe the security functional requirements of the TOE, the family FAU_SAS of the class FAU (Security audit) is defined here. This family describes the functional requirements for the storage of audit data. It has a more general approach than FAU_GEN, because it does not necessarily require the data to be generated by the TOE itself and because it does not give specific details of the content of the audit records.

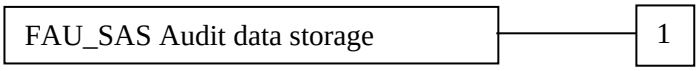
The family 'Audit data storage (FAU_SAS)' is specified as follows:

FAU_SAS Audit data storage

Family behaviour

This family defines functional requirements for the storage of audit data.

Component levelling



FAU_SAS.1	Requires the TOE to provide the possibility to store audit data.
Management:	FAU_SAS.1 There are no management activities foreseen.
Audit:	FAU_SAS.1 There are no actions defined to be auditable.
FAU_SAS.1	**Audit storage**
Hierarchical to:	No other components
Dependencies:	No dependencies
FAU_SAS.1.1	The TSF shall provide [assignment: *authorised users*] with the capability to store [assignment: *list of audit information*] in the audit records.

- FCS_RND.1 from the family FCS_RND from [PACEPP]

To describe the IT security functional requirements of the TOE, the family FCS_RND of the class FCS (Cryptographic support) is defined here. This family describes the

functional requirements for random number generation used for cryptographic purposes. The component FCS_RND.1 is not limited to generation of cryptographic keys unlike the component FCS_CKM.1. The similar component FIA_SOS.2 is intended for non-cryptographic use.

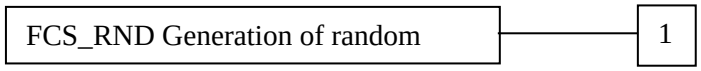
The family 'Generation of random numbers (FCS_RND)' is specified as follows:

FCS_RND Generation of random numbers

Family behaviour

This family defines quality requirements for the generation of random numbers intended to be used for cryptographic purposes.

Component levelling:



FCS_RND.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RND.1 There are no management activities foreseen.
Audit:	FCS_RND.1 There are no actions defined to be auditable.
FCS_RND.1	**Quality metric for random numbers**
Hierarchical to:	No other components
Dependencies:	No dependencies
FCS_RND.1.1	The TSF shall provide a mechanism to generate random numbers that meet [assignment: *a defined quality metric*].

- FMT_LIM.1 and FMT_LIM.2 from the family FMT_LIM from [PACEPP]

The family FMT_LIM describes the functional requirements for the test features of the TOE. The new functional requirements were defined in the class FMT because this class addresses the management of functions of the TSF. The examples of the technical mechanism used in the TOE show that no other class is appropriate to address the specific issues of preventing abuse of functions by limiting the capabilities of the functions and by limiting their availability.

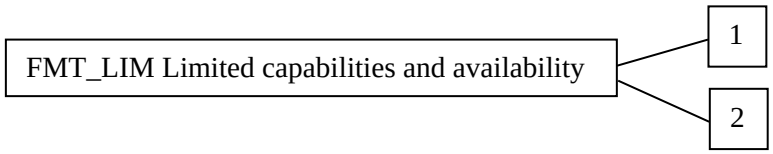
The family 'Limited capabilities and availability (FMT_LIM)' is specified as follows:

FMT_LIM Limited capabilities and availability

Family behaviour

This family defines requirements that limit the capabilities and availability of functions in a combined manner. Note, that FDP_ACF restricts access to functions whereas the Limited capability of this family requires the functions themselves to be designed in a specific manner.

Component levelling:



FMT_LIM.1	Limited capabilities requires that the TSF is built to provide only the capabilities (perform action, gather information) necessary for its genuine purpose.
FMT_LIM.2	Limited availability requires that the TSF restrict the use of functions (refer to Limited capabilities (FMT_LIM.1)). This can be achieved, for instance, by removing or by disabling functions in a specific phase of the TOE's life-cycle.
Management:	FMT_LIM.1, FMT_LIM.2 There are no management activities foreseen.
Audit:	FMT_LIM.1, FMT_LIM.2 There are no actions defined to be auditable.

FMT_LIM.1	**Limited capabilities**
Hierarchical to:	No other components
Dependencies:	FMT_LIM.2 Limited availability
FMT_LIM.1.1	The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2)' the following policy is enforced [assignment: *Limited capability and availability policy*].
FMT_LIM.2	**Limited availability**
Hierarchical to:	No other components

Dependencies: FMT_LIM.1 Limited capabilities

FMT_LIM.2.1 The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1)' the following policy is enforced [assignment: *Limited capability and availability policy*].

Application note 28*:* The functional requirements FMT_LIM.1 and FMT_LIM.2 assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

i. the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced

or conversely

ii. (ii)the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

- FPT_EMS.1 from the family FPT_EMS from [PACEPP] and [SSCDPP]

The family FPT_EMS (TOE Emanation) of the class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against secret data stored in and used by the TOE where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc. This family describes the functional requirements for the limitation of intelligible emanations being not directly addressed by any other component of CC part 2 [CC].

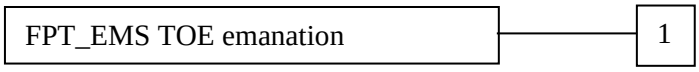
The family 'TOE Emanation (FPT_EMS)' is specified as follows:

FPT_EMS TOE emanation

Family behaviour

This family defines requirements to mitigate intelligible emanations.

Component levelling:



FPT_EMS.1 TOE emanation has two constituents:

FPT_EMS.1.1 Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.

FPT_EMS.1.2 Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions defined to be auditable.

FPT_EMS.1 TOE Emanation

Hierarchical to: No other components

Dependencies: No dependencies

FPT_EMS.1.1 The TOE shall not emit [assignment: *types of emissions*] in excess of [assignment: *specified limits*] enabling access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

FPT_EMS.1.2 The TSF shall ensure [assignment: *type of users*] are unable to use the following interface [assignment: *type of connection*] to gain access to [assignment: *list of types of TSF data*] and [assignment: *list of types of user data*].

- FIA_API.1 from the family FIA_API from [EAC2PP]

To describe the IT security functional requirements of the TOE, the family FIA_API of the class FIA (Identification and authentication) is defined here. This family describes the functional requirements for proof of the claimed identity for the authentication verification by an external entity, where the other families of the class FIA address the verification of the identity of an external entity.

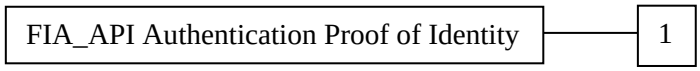
Application note 29: Other families of the class FIA describe only the authentication verification of the user's identity performed by the TOE and do not describe the functionality of the TOE to prove its own identity. The following paragraph defines the family FIA_API in the style of Common Criteria part 2 (cf. CC part 3 [CC], chapter 'Extended components definition (APE_ECD)') from a TOE point of view.

FIA_API Authentication Proof of Identity

Family behaviour

This family defines functions provided by the TOE to prove its identity and to be verified by an external entity in the TOE IT environment.

Component levelling:



FIA_API.1 Authentication Proof of Identity.

Management FIA_API.1

The following actions could be considered for the management functions in FMT: Management of authentication information used to prove the claimed identity.

Audit: FIA_API.1

There are no actions defined to be auditable.

FIA_API.1 Authentication Proof of Identity

Hierarchical to: No other components

Dependencies: No dependencies

FIA_API.1.1 The TSF shall provide a [assignment: *authentication mechanism*] to prove the identity of the [assignment: *authorised user or role, or of the TOE itself*].

7. Security Requirements

This part defines detailed security requirements that shall be satisfied by the TOE. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE must satisfy in order to meet the security objectives for the TOE.

Common Criteria allows several operations to be performed on security requirements on the component level: refinement, selection, assignment and iteration, cf. sec. 8.1 of CC part 1 [CC]. Each of these operations is used in this ST.

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinements of security requirements made by the PP author are denoted in such a way that added words are in **bold text** and removed are ~~crossed out~~. Refinements made by the ST author appear *italicized*, **bold** and underlined and ~~crossed out~~ if text is removed.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections having been made by the PP author are denoted as underlined text. Selections made by the ST author appear *italicized and* underlined.

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignments having been made by the PP author are denoted by showing as underlined text. Assignments made by the ST author appear *italicized* and underlined.

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier. For the sake of better readability, the iteration operation may also be applied to a non-repeated single component in order to indicate that such component belongs to a certain functional cluster. In such a case, the iteration operation is applied to only one single component.

In order to distinguish between SFRs defined here and SFRs that are taken over from PPs to which this ST claims strict conformance, the latter are iterated resp. renamed in the following way:

/EAC1PP or /XXX_EAC1PP [EAC1PP],

/EAC2PP or /XXX_EAC2PP for [EAC2PP],

/SSCDPP or /XXX_SSCDPP for [SSCDPP].

/SSCDPP4 or /XXX_SSCDPP4 for [SSCDPP4].

and /SSCDPP5 or /XXX_SSCDPP5 for [SSCDPP5].

The definition of the subjects "Manufacturer", "Personalisation Agent", "Extended Inspection System", "Country Verifying Certification Authority", "Document Verifier" and "Terminal" used

in the following chapter is given in section 3.1. Note, that all these subjects are acting for homonymous external entities. All used objects are defined either in section 7 or in the following table. The operations “write”, “modify”, “read” and “disable read access” are used in accordance with the general linguistic usage. The operations “store”, “create”, “transmit”, “receive”, “establish communication channel”, “authenticate” and “re-authenticate” are originally taken from [CC]. The operation “load” is synonymous to “import” used in [CC].

Definition of security attributes:

security attribute	**values**	**meaning**
terminal authentication status	none (any Terminal)	default role (i.e. without authorisation after start-up)
	CVCA	roles defined in the certificate used for authentication (cf. [TR03110]); Terminal is authenticated as Country Verifying Certification Authority after successful CA and TA
	DV (domestic)	roles defined in the certificate used for authentication (cf. [TR03110]); Terminal is authenticated as domestic Document Verifier after successful CA and TA
	DV (foreign)	roles defined in the certificate used for authentication (cf. [TR03110]); Terminal is authenticated as foreign Document Verifier after successful CA and TA
	IS	roles defined in the certificate used for authentication (cf. [TR03110]); Terminal is authenticated as Extended Inspection System after successful CA and TA
Terminal Authorization	none	
	DG4 (Iris)	Read access to DG4: (cf. [TR03110])
	DG3 (Fingerprint)	Read access to DG3: (cf. [TR03110])
	DG3 (Fingerprint) / DG4 (Iris)	Read access to DG3 and DG4: (cf. [TR03110])

Tabla 3.- Definition of security attributes.

The following table provides an overview of the keys and certificates used. Further keys and certificates are listed in [PACEPP].

Name	**Data**
TOE intrinsic secret cryptographic keys	Permanently or temporarily stored secret cryptographic material used by the TOE in order to enforce its security functionality.
Country Verifying Certification Authority Private	The Country Verifying Certification Authority (CVCA) holds a private key (SK_{CVCA}) used for signing the Document Verifier

Key (SK_{CVCA})	Certificates.
Country Verifying Certification Authority Public Key (PK_{CVCA})	The TOE stores the Country Verifying Certification Authority Public Key (PK_{CVCA}) as part of the TSF data to verify the Document Verifier Certificates. The PK_{CVCA} has the security attribute Current Date as the most recent valid effective date of the Country Verifying Certification Authority Certificate or of a domestic Document Verifier Certificate.
Country Verifying Certification Authority Certificate (C_{CVCA})	The Country Verifying Certification Authority Certificate may be a self-signed certificate or a link certificate (cf. [TR03110] and Glossary). It contains (i) the Country Verifying Certification Authority Public Key (PK_{CVCA}) as authentication reference data, (ii) the coded access control rights of the Country Verifying Certification Authority, (iii) the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Document Verifier Certificate (C_{DV})	The Document Verifier Certificate C_{DV} is issued by the Country Verifying Certification Authority. It contains (i) the Document Verifier Public Key (PK_{DV}) as authentication reference data (ii) identification as domestic or foreign Document Verifier, the coded access control rights of the Document Verifier, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Inspection System Certificate (C_{IS})	The Inspection System Certificate (C_{IS}) is issued by the Document Verifier. It contains (i) as authentication reference data the Inspection System Public Key (PK_{IS}), (ii) the coded access control rights of the Extended Inspection System, the Certificate Effective Date and the Certificate Expiration Date as security attributes.
Chip Authentication Public Key Pair	The Chip Authentication Public Key Pair (SK_{ICC}, PK_{ICC}) are used for Key Agreement Protocol: Diffie-Hellman (DH) according to RFC 2631 or Elliptic Curve Diffie-Hellman according to ISO 11770-3 [ISO11770].
Chip Authentication Public Key (PK_{ICC})	The Chip Authentication Public Key (PK_{ICC}) is stored in the EF.DG14 Chip Authentication Public Key of the TOE's logical travel document and used by the inspection system for Chip Authentication Version 1 of the travel document's chip. It is part of the user data provided by the TOE for the IT environment.
Chip Authentication Private Key (SK_{ICC})	The Chip Authentication Private Key (SK_{ICC}) is used by the TOE to authenticate itself as authentic travel document's chip. It is part of the TSF data.
Country Signing Certification Authority Key Pair	Country Signing Certification Authority of the issuing State or Organisation signs the Document Signer Public Key Certificate with the Country Signing Certification Authority Private Key and the signature will be verified by receiving State or Organisation (e.g. an Extended Inspection System) with the Country Signing Certification Authority Public Key.

Document Signer Key Pairs	Document Signer of the issuing State or Organisation signs the Document Security Object of the logical travel document with the Document Signer Private Key and the signature will be verified Organisation with the Document Signer Public Key.
Chip Authentication Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of the Chip Authentication Protocol Version 1.
PACE Session Keys	Secure messaging encryption key and MAC computation key agreed between the TOE and an Inspection System in result of PACE.

Tabla 4.- Keys and certificates.

Application note 30: The Country Verifying Certification Authority identifies a Document Verifier as “domestic” in the Document Verifier Certificate if it belongs to the same State as the Country Verifying Certification Authority. The Country Verifying Certification Authority identifies a Document Verifier as “foreign” in the Document Verifier Certificate if it does not belong to the same State as the Country Verifying Certification Authority. From travel document’s point of view the domestic Document Verifier belongs to the issuing State or Organisation.

7.1. Security Functional Requirements

The statements of security requirements must be internally consistent. As several different PPs with similar SFRs are claimed, great care must be taken to ensure that these several iterated SFRs do not lead to inconsistency.

Both [EAC1PP] and [EAC2PP] claim strict conformance to [PACEPP]. Thus they include all SFRs from [PACEPP]. On the other hand, due to strict conformance to [EAC1PP] and [EAC2PP], this ST includes all SFRs from [EAC1PP] and [EAC2PP] except FIA_API.1/RI. **Hence all SFRs from [PACEPP] appear in this ST twice as SFRs from [EAC1PP] and [EAC2PP], and thus SFRs from [PACEPP] are not listed in this ST. In other words, despite claiming strict conformance to [PACEPP], SFRs can be safely ignored during evaluation and certification as long as [EAC1PP] and [EAC2PP] are taken into account.**

One must remember that each of these iterated SFRs mostly concerns different (groups of) user and TSF data for each protocol (i.e. PACE, EAC1 and EAC2). We distinguish three cases:

1. The SFRs apply to different data that are accessible by executing different protocols. Hence, they are completely separate. An example is FCS_CKM.1/DH_PACE from [EAC1PP] and [EAC2PP]. No remark is added in such case in the text below.
2. The SFRs are equivalent. Then we list them all for the sake of completeness. Hence, it suffices to consider only one iteration. For such SFRs, we explicitly give a remark. An example is FIA_AFL.1/PACE from [EAC1PP] and [EAC2PP].

3. The SFRs do not apply to different data or protocols, but are also not completely equivalent. Then these multiple SFRs are refined in such a way, that one common component is reached that subsumes all iterations that stem from the inclusions of the claimed PPs. An example is FDP_ACF.1, which is combined here from [EAC1PP] and [EAC2PP]. Such a case is also explicitly mentioned in the text.

Thus internal consistency is not violated.

Last, we remark that compared to [EAC2PP] the following references in SFRs have been updated:

- The reference [ICAO9303] was updated from the sixth to the seventh edition.
- The document *Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.1, 15. April 2014*. was replaced with [ICAO9303], since that technical report has been included in the seventh edition of [ICAO9303].

Since the content of the specifications has not changed, we do not explicitly mark these (editorial) refinements in the SFRs.

7.1.1. Class FCS

7.1.1.1. Class FCS from [MR.ED-ON-PP]

FCS_COP.1/UPD_ITC Cryptographic Operation – Inter Trusted Channel

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/UPD_ITC

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/UPD

FCS_COP.1.1/UPD_ITC The TSF shall perform *secure messaging – encryption and decryption*[22] in accordance with a specified cryptographic algorithm *AES in CBC mode*[23] and cryptographic key sizes *192 bits*[24] that meet the following: *[EN419212-3]*[25].

FCS_CKM.1/UPD_ITC Cryptographic Key Generation

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

fulfilled by FCS_COP.1/UPD_ITC

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/UPD

FCS_CKM.1.1/UPD_ITC The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *Section 3.8.3 of [EN419212-3]*[26] and specified cryptographic key sizes *192 bits*[27] that meet the following: *[EN419212-3]*[28].

FCS_COP.1/UPD_DEC Cryptographic Operation – Decryption of Update Packages

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

[22] [assignment: *list of cryptographic operations*]
[23] [assignment: *cryptographic algorithm*]
[24] [assignment: *cryptographic key sizes*]
[25] [assignment: *list of standards*]
[26] [assignment: *cryptographic key generation algorithm*]
[27] [assignment: *cryptographic key sizes*]
[28] [assignment: *list of standards*]

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/UPD_DEC

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/UPD

FCS_COP.1.1/UPD_DEC	The TSF shall perform *decryption of update packages*[29] in accordance with a specified cryptographic algorithm *AES*[30] and cryptographic key sizes *128 bits*[31] that meet the following: *none*[32].

FCS_CKM.1/UPD_DEC **Cryptographic Key Generation**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

fulfilled by FCS_COP.1/UPD_DEC

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/UPD

FCS_CKM.1.1/UPD_DEC	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES*[33] and specified cryptographic key sizes *128 bits*[34] that meet the following: *none*[35].

[29] [assignment: *list of cryptographic operations*]
[30] [assignment: *cryptographic algorithm*]
[31] [assignment: *cryptographic key sizes*]
[32] [assignment: *list of standards*]
[33] [assignment: *cryptographic key generation algorithm*]
[34] [assignment: *cryptographic key sizes*]
[35] [assignment: *list of standards*]

FCS_COP.1/UPD_SIG **Cryptographic Operation – Signature Verification of Update Packages**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

not fulfilled but justified: The TOE uses security attributes (keys) that have been defined during the personalization and are fixed over the whole life time of the TOE. No import or generation of these security attributes is necessary here.

FCS_CKM.4 Cryptographic key destruction

not fulfilled but justified: The TOE uses security attributes (keys) that have been defined during the personalization and are fixed over the whole life time of the TOE. Key destruction implies not being able to verify digital signatures from then on, and hence, is not applicable here.

FCS_COP.1.1/UPD_SIG The TSF shall perform *digital signature verification*[36] in accordance with a specified cryptographic algorithm *RSA or ECDSA*[37] and cryptographic key sizes *3072 – 3840 bits (for RSA) or 256 bits, 384 bits, 512 bits and 521 bits (for ECDSA)*[38] that meet the following: *[PKCS#1] v2.1 RFC 3447 or The Elliptic Curve Digital Signature Algorithm (ECDSA) American National Standards Institute, ANSI, 2005*[39].

FCS_COP.1/UPD_INT **Cryptographic Operation – Integrity Verification of Update Package**

[36] [assignment: *list of cryptographic operations*]
[37] [assignment: *cryptographic algorithm*]
[38] [assignment: *cryptographic key sizes*]
[39] [assignment: *list of standards*]

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/UPD_INT

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/UPD

FCS_COP.1.1/UPD_INT	The TSF shall perform *integrity verification of update packages*[40] in accordance with a specified cryptographic algorithm *CMAC*[41] and cryptographic key sizes *128 bits*[42] that meet the following: *NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005*[43].

Application note 31: Integrity verification of packages is intended to be used for a hash function (keyed or unkeyed) with which the TOE checks the integrity of received update packages prior to decryption.

FCS_CKM.1/UPD_INT Cryptographic Key Generation

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation]

fulfilled by FCS_COP.1/UPD_INT

[40] [assignment: *list of cryptographic operations*]
[41] [assignment: *cryptographic algorithm*]
[42] [assignment: *cryptographic key sizes*]
[43] [assignment: *list of standards*]

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/UPD

FCS_CKM.1.1/UPD_INT The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES*[44] and specified cryptographic key sizes *128 bits*[45] that meet the following: *none*[46].

Application note 32: This SFR is intended for the key generation in case a keyed hash function is used for FCS_COP.1/UPD_INT. In case of an unkeyed hash function is used, the integrity is solely implied by digital signature verification. Hence in this case, 'none' is assigned.

FCS_CKM.4/UPD_OS Cryptographic Key Destruction – Operating System

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]:

fulfilled by FCS_CKM.1/UPD_DEC and FCS_CKM.1/UPD_ITC

FCS_CKM.4.1/UPD_OS The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroes writing in the zone memory in where (AES) session key is stored*[47] that meets the following: *none*[48].

FCS_CKM.4/UPD Cryptographic Key Destruction

[44] [assignment: *cryptographic key generation algorithm*]
[45] [assignment: *cryptographic key sizes*]
[46] [assignment: *list of standards*]
[47] [assignment: *cryptographic key destruction method*]
[48] [assignment: *list of standards*]

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]:

fulfilled by FCS_CKM.1/UPD_INT

FCS_CKM.4.1/UPD The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *Loader mechanism destruction method*[49] that meets the following: *none*[50].

7.1.1.2. Class FCS imported from [EAC2PP]

The following SFRs are imported due to claiming [EAC2PP]. They concern cryptographic support for applications that contain EAC2-protected data groups.

FCS_CKM.1/DH_PACE_EAC2PP **Cryptographic Key Generation – Diffie-Hellman for PACE and CA2 Session Keys**

Hierarchical to:

No other components

Dependencies:

[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
not fulfilled, but **justified**:
A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.
FCS_CKM.4 Cryptographic key destruction
fulfilled by FCS_CKM.4/EAC2PP

FCS_CKM.1.1/DH_PACE_EAC2PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [TR03111]*[51] and specified cryptographic

[49] [assignment: *cryptographic key destruction method*]
[50] [assignment: *list of standards*]

key sizes *256 bits, 384 bits, 512 bits and 521 bits*[52] that meet the following: *[TR03110-2] using brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 curves defined in [RFC5639] and NIST P-256, NIST P-384 and NIST P-521 curves defined in [NIST SP 800-186]*[53].

Application note 33: In the above and all subsequent related SFRs, the reference w.r.t. the PACE protocol is changed to [TR03110-2], whereas [PACEPP] references [ICAO-SAC]. The difference between the two definitions is that [TR03110-2] defines additional optional parameters for the command MSE:Set AT. This optional parameters (e.g. the CHAT) are technically required, since here Terminal Authentication 2 (TA2) can be executed right after PACE (see FIA_UID.1/EAC2_Terminal). As [ICAO-SAC] does not consider TA2, no such definition is given there. These additional parameters are optional and not used during PACE itself (only afterwards). If PACE is run without TA2 afterwards, access to data on the chip is given as specified by [PACEPP]. If TA2 is run afterwards, access to data on the chip can be further restricted w.r.t. to the authorization level of the terminal. Therefore this change of references does not violate strict conformance to [PACEPP]. We treat this change of references as a refinement operation, and thus mark the changed reference using **bold** text.

Application note 34: National cryptographic requirements may further restrict available choices in the selection of the above SFR.

Application note 35: [PACEPP] considers Diffie-Hellman key generation only for PACE. Since the TOE is required to implement Chip Authentication 2 (cf. FIA_API.1/CA_EAC2PP), here FCS_CKM.1/DH_PACE_EAC2PP applies for CA2 as well.

FCS_COP.1/SHA_EAC2PP **Cryptographic operation – Hash for key derivation**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

not fulfilled, but **justified**:

A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here.

FCS_CKM.4 Cryptographic key destruction

[51] [assignment: *cryptographic key generation algorithm*]
[52] [assignment: *cryptographic key sizes*]
[53] [assignment: *list of standards*]

not fulfilled, but **justified**:

A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.

FCS_COP.1.1/SHA_EAC2PP

The TSF shall perform hashing[54] in accordance with a specified cryptographic algorithm *SHA-256*[55] and cryptographic key sizes none[56] that meet the following: [SHS][57].

Application note 36: For compressing (hashing) an ephemeral public key for DH (TA2 and CA2), the hash function SHA-1 shall be used ([TR03110-3]). The TOE shall implement as hash functions either SHA-1 or SHA-224 or SHA-256 for Terminal Authentication 2, cf. [TR03110-3].

Within the normative Appendix of [TR03110-3] 'Key Derivation Function', it is stated that the hash function SHA-1 shall be used for deriving 128-bit AES keys, whereas SHA-256 shall be used for deriving 192-bit and 256-bit AES keys.

FCS_COP.1/SIG_VER_EAC2PP Cryptographic operation – Signature verification

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

not fulfilled, but **justified**:

The root key PK_{CVCA} (initialization data) used for verifying the DV Certificate is stored in the TOE during its personalization in the card issuing life cycle phase[58]. Since importing the respective certificates (Terminal Certificate, DV Certificate) does not require any special security measures except those required by the current SFR (cf. FMT_MTD.3/EAC2PP below), the current ST does not contain any dedicated requirement like FDP_ITC.2 for the import function.

FCS_CKM.4 Cryptographic key destruction

not fulfilled, but **justified**:

[54] [assignment: *list of cryptographic operations*]
[55] [assignment: *cryptographic algorithm*]
[56] [assignment: *cryptographic key sizes*]
[57] [assignment: *list of standards*]
[58] as already mentioned, operational use of the TOE is explicitly in focus of the current ST.

Cryptographic keys used for the purpose of the current SFR (PK_{PCD}, PK_{DV}, PK_{CVCA}) are public keys; they do not represent any secret, and hence need not to be destroyed.

FCS_COP.1.1/SIG_VER_EAC2PP

The TSF shall perform digital signature verification[59] in accordance with a specified cryptographic algorithm *ECDSA*[60] and cryptographic key sizes *256 bits, 384 bits, 512 bits and 521 bits*[61] that meet the following: *The Elliptic Curve Digital Signature Algorithm (ECDSA) American National Standards Institute, ANSI, 2005*[62].

Application note 37: This SFR is concerned with Terminal Authentication 2, cf. [TR03110-2].

FCS_COP.1/PACE_ENC_EAC2PP **Cryptographic operation – Encryption / Decryption AES**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/DH_PACE_EAC2PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC2PP

FCS_COP.1.1/PACE_ENC_EAC2PP

The TSF shall perform secure messaging – encryption and decryption[63] in accordance with a specified cryptographic algorithm AES in CBC mode[64] and cryptographic key sizes *192 bits*[65] that meet the following: **[TR03110-3]**[66].

Application note 38: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed

[59] [assignment: *list of cryptographic operations*]
[60] [assignment: *cryptographic algorithm*]
[61] [assignment: *cryptographic key sizes*]
[62] [assignment: *list of standards*]
[63] [assignment: *list of cryptographic operations*]
[64] [selection: *cryptographic algorithm*]
[65] [selection: *128, 192, 256 bit*]
[66] [assignment: *list of standards*]

between the TOE and the terminal as part of either the PACE protocol (PACE-K_{Enc}) or Chip Authentication 2 (CA-K_{Enc}) according to FCS_CKM.1/DH_PACE_EAC2PP. Note that in accordance with [TR03110-3], 3DES could be used in CBC mode for secure messaging. Due to the fact that 3DES is not recommended any more (cf. [TR03116-2]), 3DES in any mode is no longer applicable here.

Application note 39: Refinement of FCS_COP.1.1/PACE_ENC_EAC2PP, since here PACE must adhere to [TR03110-3]. All references (both the one in [PACEPP] and [TR03110-3]) itself reference [ISO7816-4] for secure messaging. [TR03110-3] however further restricts the available choice of key-sizes and algorithms. Hence, [TR03110-3] is fully (backward) compatible to the reference given in [PACEPP].

FCS_COP.1/PACE_MAC_EAC2PP **Cryptographic operation – CMAC**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/DH_PACE_EAC2PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC2PP

FCS_COP.1.1/PACE_MAC_EAC2PP

The TSF shall perform secure messaging – message authentication code[67] in accordance with a specified cryptographic algorithm CMAC[68] and cryptographic key sizes *192 bits*[69] that meet the following: [**TR03110-3**][70].

Application note 40: see Application note 39.

Application note 41: This SFR removes 3DES and restricts to CMAC compared to the SFR of [PACEPP] by selection. Hence, a minimum key-size of 128 bit is required.

[67] [assignment: *list of cryptographic operations*]
[68] [selection: *cryptographic algorithm*]
[69] [selection: ~~*112*~~*,128, 192, 256 bit*]
[70] [assignment: *list of standards*]

In addition, this ST includes all remaining SFRs of [PACEPP]. For the class FCS, these are the following components:

FCS_CKM.4/EAC2PP **Cryptographic key destruction – Session keys**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/DH_PACE

FCS_CKM.4.1/EAC2PP The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroes writing in the zone memory in where (AES) session key is stored*[71] that meets the following: *none*[72].

Application note 42: The TOE shall destroy the PACE session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1/EAC2PP.

The *Application Note* above concerning this component requires the destruction of PACE session keys after detection of an error in a received command by verification of the MAC. While the definition of FCS_CKM.4/EAC2PP remains unaltered, here this component also requires the destruction of sessions keys after a successful run of Chip Authentication 2. The TOE shall destroy the CA2 session keys after detection of an error in a received command by verification of the MAC. The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1/EAC2PP.

FCS_RND.1/EAC2PP **Quality metric for random numbers**

Hierarchical to:

[71] [assignment: *cryptographic key destruction method*]
[72] [assignment: *list of standards*]

No other components.

Dependencies:

No dependencies.

FCS_RND.1.1/EAC2PP The TSF shall provide a mechanism to generate random numbers that meet *NIST Special Publication 800-90A*[73].

Application note 43: This SFR requires the TOE to generate random numbers (random nonce) used for the authentication protocol (PACE) as required by FIA_UAU.4/PACE_EAC2PP.

The *Application Note* above concerning this component requires the TOE to generate random numbers (random nonces) for PACE. While the definition of FCS_RND.1/EAC2PP remains unaltered, here this component requires the TOE to generate random numbers (random nonce) for all authentication protocols (i.e. PACE, CA2), as required by FIA_UAU.4/PACE_EAC2PP.

7.1.1.3. Class FCS imported from [EAC1PP]

The following SFRs are imported due to claiming [EAC1PP]. They concern cryptographic support for applications that contain EAC1-protected data groups.

FCS_CKM.1/DH_PACE_EAC1PP **Cryptographic key generation – Diffie-Hellman for PACE session keys**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]:

Justification: A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.

FCS_CKM.4 Cryptographic key destruction: fulfilled by FCS_CKM.4/EAC1PP

FCS_CKM.1.1/DH_PACE_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *ECDH compliant to [TR03111]*[74] and specified cryptographic

[73] [assignment: *a defined quality metric*]
[74] [selection: Diffie-Hellman-Protocol compliant to PKCS#3, ECDH compliant to [TR03111]]

key sizes *256 bits, 384 bits, 512 bits and 521 bits*[75] that meet the following: [ICAO9303] using brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 curves defined in [RFC5639] and NIST P-256, NIST P-384 and NIST P-521 curves defined in [NIST SP 800-186][76].

Application note 44: The TOE generates a shared secret value K with the terminal during the PACE protocol, see [ICAO9303]. This protocol may be based on the ECDH compliant to [TR03111] (i.e. the elliptic curve cryptographic algorithm ECKA, cf. [ICAO9303] and [TR03111] for details). The shared secret value K is used for deriving the AES session keys for message encryption and message authentication (PACE-K_{MAC}, PACE-K_{Enc}) according to [ICAO9303] for the TSF required by FCS_COP.1/PACE_ENC_EAC1PP and FCS_COP.1/PACE_MAC_EAC1PP.

Application note 45: FCS_CKM.1/DH_PACE_EAC1PP implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [ICAO9303].

FCS_CKM.4/EAC1PP

(equivalent to FCS_CKM.4/EAC2PP, but listed here for the sake of completeness)

FCS_COP.1/PACE_ENC_EAC1PP **Cryptographic operation – Encryption / Decryption AES**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]:

fulfilled by FCS_CKM.1/DH_PACE_EAC1PP

FCS_CKM.4 Cryptographic key destruction:

fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/PACE_ENC_EAC1PP

[75] [assignment: *cryptographic key sizes*]
[76] [assignment: *list of standards*]

The TSF shall perform secure messaging – encryption and decryption[77] in accordance with a specified cryptographic algorithm *AES* in CBC mode[78] and cryptographic key sizes *192 bits*[79] that meet the following: compliant to [ICAO9303][80].

Application note 46: This SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data and encrypting the nonce in the first step of PACE. The related session keys are agreed between the TOE and the terminal as part of the PACE protocol according to the FCS_CKM.1/DH_PACE_EAC1PP (PACE-KEnc).

FCS_COP.1/PACE_MAC_EAC1PP Cryptographic operation – MAC

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]:

fulfilled by FCS_CKM.1/DH_PACE_EAC1PP

FCS_CKM.4 Cryptographic key destruction:

fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/PACE_MAC_EAC1PP

The TSF shall perform secure messaging – message authentication code[81] in accordance with a specified cryptographic algorithm *CMAC*[82] and cryptographic key sizes *192 bits*[83] that meet the following: compliant to [ICAO9303][84].

Application note 47: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with message authentication code over transmitted data. The related session keys are agreed between the TOE and the terminal as part of either the PACE protocol according to the FCS_CKM.1/DH_PACE_EAC1PP (PACE-KMAC).

[77] [assignment: *list of cryptographic operations*]
[78] [assignment: *cryptographic algorithm*]
[79] [assignment: *cryptographic key sizes*]
[80] [assignment: *list of standards*]
[81] [assignment: *list of cryptographic operations*]
[82] [assignment: *cryptographic algorithm*]
[83] [assignment: *cryptographic key sizes*]
[84] [assignment: *list of standards*]

Application note 48: Note that national regulations w.r.t. key sizes and algorithms may further restrict the choice of algorithms and key sizes defined in the above two SFRs.

FCS_RND.1/EAC1PP

(equivalent to FCS_RND.1/EAC2PP, but listed here for the sake of completeness)

FCS_CKM.1/CA_EAC1PP **Cryptographic key generation – Diffie-Hellman for Chip Authentication session keys**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]

fulfilled by FCS_COP.1/CA_ENC and FCS_COP.1/CA_MAC.

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC1PP.

FCS_CKM.1.1/CA_EAC1PP

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES*[85] and specified cryptographic key sizes *192 bits*[86] that meet the following: *based on ECDH protocol compliant to [TR03110] using brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 curves defined in [RFC5639] and NIST P-256, NIST P-384 and NIST P-521 curves defined in [NIST SP 800-186]*[87].

Application note 49: FCS_CKM.1/CA_EAC1PP implicitly contains the requirements for the hashing functions used for key derivation by demanding compliance to [TR03110].

Application note 50: The TOE generates a shared secret value with the terminal during the Chip Authentication Protocol Version 1, see [TR03110]. This protocol may be based on the ECDH compliant to TR-03111 (i.e. an elliptic curve cryptography algorithm) (cf. [TR03111], for details). The shared secret value is used to derive the Chip Authentication Session Keys used

[85] [assignment: *cryptographic key generation algorithm*]
[86] [assignment: *cryptographic key sizes*]
[87] [assignment: list of standards]

for encryption and MAC computation for secure messaging (defined in Key Derivation Function [TR03110]).

Application note 51: The TOE shall implement the hash function SHA-256 for the cryptographic primitive to derive the keys for secure messaging from any shared secrets of the Authentication Mechanisms. The Chip Authentication Protocol v.1 uses SHA-256 (cf. [TR03110]). The TOE also implements the hash function SHA-256 for the Terminal Authentication Protocol v.1 (cf. [TR03110] for details).

Application note 52: The TOE shall destroy any session keys in accordance with FCS_CKM.4 from [PACEPP] after (i) detection of an error in a received command by verification of the MAC and (ii) after successful run of the Chip Authentication Protocol v.1. (iii) The TOE shall destroy the PACE Session Keys after generation of a Chip Authentication Session Keys and changing the secure messaging to the Chip Authentication Session Keys. (iv) The TOE shall clear the memory area of any session keys before starting the communication with the terminal in a new after-reset-session as required by FDP_RIP.1/EAC1PP. Concerning the Chip Authentication keys FCS_CKM.4/EAC1PP is also fulfilled by FCS_CKM.1/CA_EAC1PP.

FCS_COP.1/CA_ENC_EAC1PP **Cryptographic operation – Symmetric Encryption / Decryption**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/CA_EAC1PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/CA_ENC_EAC1PP

The TSF shall perform secure messaging – encryption and decryption[88] in accordance with a specified cryptographic algorithm *AES*[89] and cryptographic key sizes *192 bits*[90]

[88] [assignment: *list of cryptographic operations*]
[89] [assignment: *cryptographic algorithm*]
[90] [assignment: *cryptographic key sizes*]

that meet the following: *Federal Information Processing Standards (FIPS) Publication 197 [AES] and [TR03110]*[91].

Application note 53: This SFR requires the TOE to implement the cryptographic primitives (e.g. AES) for secure messaging with encryption of the transmitted data. The keys are agreed between the TOE and the terminal as part of the Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA_EAC1PP.

FCS_COP.1/SIG_VER_EAC1PP **Cryptographic operation – Signature verification by travel document**

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/CA_EAC1PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/SIG_VER_EAC1PP

The TSF shall perform digital signature verification[92] in accordance with a specified cryptographic algorithm *ECDSA*[93] and cryptographic key sizes *256 bits, 384 bits, 512 bits and 521 bits*[94] that meet the following: *The Elliptic Curve Digital Signature Algorithm (ECDSA) American National Standards Institute, ANSI, 2005*[95].

Application note 54: The ST has performed the missing operation of the assignments for the signature algorithms key lengths and standards implemented by the TOE for the Terminal Authentication Protocol v.1 (cf. [TR03110]). The signature verification is used to verify the card

[91] [assignment: *list of standards*]
[92] [assignment: *list of cryptographic operations*]
[93] [assignment: *cryptographic algorithm*]
[94] [assignment: *cryptographic key sizes*]
[95] [assignment: *list of standards*]

verifiable certificates and the authentication attempt of the terminal creating a digital signature for the TOE challenge.

FCS_COP.1/CA_MAC_EAC1PP Cryptographic operation – MAC

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/CA_EAC1PP

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/EAC1PP.

FCS_COP.1.1/CA_MAC_EAC1PP

The TSF shall perform secure messaging – message authentication code[96] in accordance with a specified cryptographic algorithm *CMAC*[97] and cryptographic key sizes *192 bits*[98] that meet the following: *NIST. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, 2005*[99].

Application note 55: This SFR requires the TOE to implement the cryptographic primitive for secure messaging with encryption and message authentication code over the transmitted data. The key is agreed between the TSF by Chip Authentication Protocol Version 1 according to the FCS_CKM.1/CA_EAC1PP. Furthermore the SFR is used for authentication attempts of a terminal as Personalisation Agent by means of the authentication mechanism.

7.1.1.4. Class FCS from [SSCDPP]

The following SFRs are imported due to claiming [SSCDPP]. They only concern the cryptographic support for an *eSign* application.

[96] [assignment: *list of cryptographic operations*]
[97] [assignment: *cryptographic algorithm*]
[98] [assignment: *cryptographic key sizes*]
[99] [assignment: *list of standards*]

FCS_CKM.1/RSA_SSCDPP **Cryptographic key generation - RSA**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] fulfilled by FCS_COP.1/RSA_SSCDPP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/RSA_SSCDPP

FCS_CKM.1.1/RSA_SSCDPP The TSF shall generate **an SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm *RSA*[100] and specified cryptographic key sizes *3072 – 3840 bits*[101] that meet the following: *[FIPS 186-4] and [FIPS 140-2]*[102].

FCS_CKM.1/EC_SSCDPP **Cryptographic key generation - EC**

Hierarchical to:

No other components.

Dependencies:

[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] fulfilled by FCS_COP.1/EC_SSCDPP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EC_SSCDPP

FCS_CKM.1.1/EC_SSCDPP The TSF shall generate ***SCD/SVD*** in accordance with a specified cryptographic key generation algorithm *Appendix A.4.3 in*

[100] [assignment: *cryptographic key generation algorithm*]
[101] [assignment: *cryptographic key sizes*]
[102] [assignment: *list of standards*]

[ANSI X9.62] and section 6.1 in [ISO15946-1][103] and specified cryptographic key sizes *256 bits, 384 bits, 512 bits and 521 bits*[104] that meet the following: *[ANSI X9.62]*[105].

FCS_CKM.4/RSA_SSCDPP Cryptographic key destruction - RSA

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/RSA_SSCDPP

FCS_CKM.4.1/RSA_SSCDPP The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroes writing in the zone memory in where SCD/SVD is stored*[106] that meets the following: *none*[107].

FCS_CKM.4/EC_SSCDPP Cryptographic key destruction - EC

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/EC_SSCDPP

[103] [assignment: *cryptographic key generation algorithm*]
[104] [assignment: *cryptographic key sizes*]
[105] [assignment: *list of standards*]
[106] [assignment: *cryptographic key destruction method*]
[107] [assignment: *list of standards*]

FCS_CKM.4.1/EC_SSCDPP The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroes writing in the zone memory in where SCD/SVD is stored*[108] that meets the following: *none*[109].

FCS_COP.1/RSA_SSCDPP Cryptographic operation - RSA

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/RSA_SSCDPP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/RSA_SSCDPP

FCS_COP.1.1/RSA_SSCDPP The TSF shall perform digital signature-generation[110] in accordance with a specified cryptographic algorithm *RSA*[111] and cryptographic key size *3072 – 3840 bits*[112] that meet the following: *[PKCS#1] v2.1 RFC 3447*[113].

FCS_COP.1/SHA_SSCDPP Cryptographic operation - SHA

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

[108] [assignment: *cryptographic key destruction method*]
[109] [assignment: *list of standards*]
[110] [assignment: *list of cryptographic operations*]
[111] [assignment: *cryptographic algorithm*]
[112] [assignment: *cryptographic key sizes*]
[113] [assignment: *list of standards*]

FCS_CKM.1 Cryptographic key generation]: not fulfilled but justified

FCS_CKM.4 Cryptographic key destruction: not fulfilled but justified

A hash function does not use any cryptographic key; hence, neither a respective key import nor key generation can be expected here.

A hash function does not use any cryptographic key; hence, a respective key destruction cannot be expected here.

FCS_COP.1.1/SHA_SSCDPP The TSF shall perform ***hash-value calculation of user chosen data***[114] in accordance with a specified cryptographic algorithm *SHA-256*[115] and cryptographic key sizes *of none*[116] that meet the following: *Federal Information Processing Standards (FIPS) Publication 180-4 [SHS]*[117].

FCS_COP.1/EC_SSCDPP Cryptographic key operation - EC

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/EC_SSCDPP

FCS_CKM.4 Cryptographic key destruction fulfilled by FCS_CKM.4/EC_SSCDPP

FCS_COP.1.1/EC_SSCDPP[118] The TSF shall perform digital signature-generation[119] in accordance with a specified cryptographic algorithm *Appendix A.4.3 in [ANSI X9.62] and section 6.1 in [ISO15946-1]*[120] and cryptographic key sizes *256 bits, 384 bits, 512 bits and 521*

[114] [assignment: *list of cryptographic operations*]
[115] [assignment: *cryptographic algorithm*]
[116] [assignment: *cryptographic key sizes*]
[117] [assignment: *list of standards*]
[118] on Weierstrass curves
[119] [assignment: *list of cryptographic operations*]
[120] [assignment: *cryptographic algorithm*]

bits[121] that meet the following: *[ANSI X9.62] using brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 curves defined in [RFC5639] and NIST P-256, NIST P-384 and NIST P-521 curves defined in [NIST SP 800-186]*[122].

7.1.1.5. Class FCS for PRO secure channel

FCS_CKM.1/AES_PRO **Cryptographic key generation – AES session keys for PRO secure channel**

Hierarchical to:

No other components

Dependencies:

[FCS_CKM.2 Cryptographic key distribution or FCS_COP.1 Cryptographic operation]
not fulfilled, but **justified**:
A Diffie-Hellman key agreement is used in order to have no key distribution, therefore FCS_CKM.2 makes no sense in this case.
FCS_CKM.4 Cryptographic key destruction
fulfilled by FCS_CKM.4/AES_PRO

FCS_CKM.1.1/AES_PRO

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *AES*[123] and specified cryptographic key sizes *192 bits*[124] that meet the following: *based on ECDH protocol compliant to [EN419212-3]*[125] *using brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 curves defined in [RFC5639] and NIST P-256, NIST P-384 and NIST P-521 curves defined in [NIST SP 800-186]*.

FCS_CKM.4/AES_PRO Cryptographic key destruction - AES

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or

[121] [assignment: *cryptographic key sizes*]
[122] [assignment: *list of standards*]
[123] [assignment: *cryptographic key generation algorithm*]
[124] [assignment: *cryptographic key sizes*]
[125] [assignment: *list of standards*]

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation] fulfilled by FCS_CKM.1/AES_PRO

FCS_CKM.4.1/AES_PRO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method *zeroes writing in the zone memory in where (AES) session key is stored*[126] that meets the following: *none*[127].

FCS_COP.1/AES_PRO Cryptographic operation - AES

Hierarchical to:

No other components.

Dependencies:

[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]

fulfilled by FCS_CKM.1/AES_PRO

FCS_CKM.4 Cryptographic key destruction

fulfilled by FCS_CKM.4/AES_PRO

FCS_COP.1.1/AES_PRO

The TSF shall perform secure messaging – encryption and decryption[128] in accordance with a specified cryptographic algorithm AES in CBC mode[129] and cryptographic key sizes *192 bits*[130] that meet the following: *[EN419212-3]*[131].

Note that this SFR requires the TOE to implement the cryptographic primitive AES for secure messaging with encryption of transmitted data. The related session keys are agreed between the TOE and the terminal as part of an elliptic curve Diffie-Hellman key agreement according to FCS_CKM.1/AES_PRO, using brainpoolP256r1, brainpoolP384r1 and brainpoolP512r1 curves defined in [RFC5639] and NIST P-256, NIST P-384 and NIST P-521 curves defined in [NIST SP 800-186].

[126] [assignment: *cryptographic key destruction method*]
[127] [assignment: *list of standards*]
[128] [assignment: *list of cryptographic operations*]
[129] [selection: *cryptographic algorithm*]
[130] [selection: *128, 192, 256 bit*]
[131] [assignment: *list of standards*]

7.1.2. Class FIA

Tabla 5 provides an overview of the authentication and identification mechanisms used.

Name	SFR for the TOE
Authentication mechanisms related to applications with EAC2-protected data	FIA_AFL.1/Suspend_PIN_EAC2PP FIA_AFL.1/Block_PIN_EAC2PP FIA_API.1/CA_EAC2PP FIA_UID.1/PACE_EAC2PP FIA_UID.1/EAC2_Terminal_EAC2PP FIA_UAU.1/PACE_EAC2PP FIA_UAU.1/EAC2_Terminal_EAC2PP FIA_UAU.4/PACE_EAC2PP FIA_UAU.5/PACE_EAC2PP FIA_UAU.6/CA_EAC2PP FIA_AFL.1/PACE_EAC2PP FIA_UAU.6/PACE_EAC2PP
Authentication mechanisms related to applications with EAC1-protected data	FIA_UID.1/PACE_EAC1PP FIA_UAU.1/PACE_EAC1PP FIA_UAU.4/PACE_EAC1PP FIA_UAU.5/PACE_EAC1PP FIA_UAU.6/PACE_EAC1PP FIA_UAU.6/EAC_EAC1PP FIA_API.1/EAC1PP FIA_AFL.1/PACE_EAC1PP
Authetication mechanisms for updating the TOE	FIA_AFL.1/UPD FIA_UAU.1/UPD FIA_UID.1/UPD
Access mechanisms for an eSign application	FIA_UID.1/SSCDPP FIA_API.1.1/SSCDPP4 FIA_AFL.1/SSCDPP FIA_AFL.1/BIO_SSCDPP

Tabla 5.- Overview of authentication SFRs

7.1.2.1. SFRs for from [MR.ED-ON-PP]

FIA_AFL.1/UPD **Update Package Verification Failure Handling**

Hierarchical to:

No other components.

Dependencies:

FIA_UAU.1 Timing of authentication:

fulfilled by FIA_UAU.1/UPD

FIA_AFL.1.1/UPD — The TSF shall detect when *3*[132] unsuccessful ~~***authentication***~~ ***update attempts*** occur~~s~~ related to *the digital signature verification*[133].

FIA_AFL.1.2/UPD — When the defined number of unsuccessful ~~***authentication***~~ ***update attempts*** has been met[134], the TSF shall *block the update mechanism*[135].

Application note 56: The above SFR is slightly refined here by replacing 'authentication' with 'update'. Also the second assignment is made more precise. An update attempt includes authentication of the update terminal to the TOE. But when a properly authenticated terminal sends an update package that is not authentic or whose integrity cannot be validated, this is still a failed update attempt, and the TOE must handle it according to the above SFR. Hence this refinement is stricter than the original SFR definition.

FIA_UID.1/UPD **Timing of Identification**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/UPD — The TSF shall allow

1) *to establish a communication channel,*
2) *to authenticate an update terminal by a successful establishment of a secure channel according to [EN419212-3]*[136]
3) *none*[137]

on behalf of the user to be performed before the user is identified.

[132] [assignment: *positive integer number*]
[133] [assignment: *list of ~~authentication~~ events of the update procedure*]
[134] [selection: *met, surpassed*]
[135] *[assignment: list of actions]*
[136] [assignment: *cryptographic method*]
[137] [assignment: *list of TSF-mediated actions*]

FIA_UID.1.2/UPD	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1/UPD **Timing of Authentication**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of Identification

fulfilled by FIA_UID.1/UPD

FIA_UAU.1.1/UPD	The TSF shall allow *1) to establish a communication channel,* *2) to authenticate an update terminal by a successful establishment of a secure channel according to [EN419212-3][138]* *3) to authenticate an update terminal by a successful establishment of a secure channel with the loader.[139]* on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/UPD	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.2.2. SFRs for EAC2-protected Data [EAC2PP]

The following SFRs are imported due to claiming [EAC2PP]. They mainly concern authentication mechanisms related to applications with EAC2-protected data.

FIA_AFL.1/Suspend_PIN_EAC2PP **Authentication failure handling – Suspending PIN**

Hierarchical to: No other components.

[138] [assignment: *cryptographic method*]
[139] [assignment: *list of TSF-mediated actions*]

Dependencies:	FIA_UAU.1 Timing of authentication fulfilled by FIA_UAU.1/PACE_EAC2PP
FIA_AFL.1.1/Suspend_PIN_EAC2PP	The TSF shall detect when *2*[140] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the PIN as the shared password for PACE[141].
FIA_AFL.1.2/Suspend_PIN_EAC2PP	When the defined number of unsuccessful authentication attempts has been met[142], the TSF shall suspend the reference value of the PIN according to [TR03110-2][143].

Application note 57: This SFR is not in conflict to FIA_AFL.1 from [PACEPP], since it just adds a requirement specific to the case where the PIN is the shared password. Thus the assigned integer number for unsuccessful authentication attempts with any PACE password could be different to the integer for the case when using a PIN.

FIA_AFL.1/Block_PIN_EAC2PP	**Authentication failure handling – Blocking PIN**
Hierarchical to:	No other components.
Dependencies:	FIA_UAU.1 Timing of authentication: fulfilled by FIA_UAU.1/PACE_EAC2PP
FIA_AFL.1.1/Block_PIN_EAC2PP	The TSF shall detect when *3*[144] unsuccessful authentication attempts occur related to consecutive failed authentication attempts using the suspended[145] PIN as the shared password for PACE[146].

[140] [selection: [assignment: *positive integer number], an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
[141] [assignment: *list of authentication events*]
[142] [selection: *met , surpassed*]
[143] [assignment: *list of actions*]
[144] [selection: [assignment: *positive integer number], an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
[145] as required by FIA_AFL.1/Suspend_PIN_EAC2PP
[146] [assignment: *list of authentication events*]

FIA_AFL.1.2/Block_PIN_EAC2PP	When the defined number of unsuccessful authentication attempts has been met[147], the TSF shall block the reference value of PIN according to [TR03110-2][148].

FIA_API.1/CA_EAC2PP	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/CA_EAC2PP	The TSF shall provide the protocol Chip Authentication 2 according to [TR03110-2][149], to prove the identity of the TOE[150].

FIA_UID.1/PACE_EAC2PP	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/PACE_EAC2PP	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE protocol according to **[TR03110-2]** 3. to read the Initialization Data if it is not disabled by TSF according to ***FMT_MTD.1/INI_DIS_EAC2PP***[151] 4. *none*[152]

[147] [selection: *met , surpassed*]
[148] [assignment: *list of actions*]
[149] [assignment: *authentication mechanism*]
[150] [assignment: *authorised user or role, or of the TOE itself*]
[151] [assignment: *list of TSF-mediated actions*]
[152] [assignment: *list of TSF-mediated actions*]

	on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/PACE_EAC2PP	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note 58: The user identified after a successful run of PACE is a PACE terminal. In case the PIN or PUK were used for PACE, the user identified is the electronic document holder using a PACE terminal. Note that neither the CAN nor the MRZ effectively represent secrets, but are restricted-revealable; i.e. in case the CAN or the MRZ were used for PACE, it is either the electronic document holder itself, an authorized person other than the electronic document holder, or a device.

FIA_UID.1/EAC2_Terminal_EAC2PP	**Timing of identification**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/EAC2_Terminal_EAC2PP	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE protocol according to [TR03110-2] , 3. to read the Initialization Data if it is not disabled by TSF according to ***FMT_MTD.1/INI_DIS_EAC2PP*** 4. carrying out the Terminal Authentication protocol 2 according to [TR03110-2][153] 5. *none*[154] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2/EAC2_Terminal_EAC2PP	The TSF shall require each user to be successfully identified before allowing any

[153] [assignment: *list of TSF-mediated actions*]
[154] [assignment: *list of TSF-mediated actions*]

other TSF-mediated actions on behalf of that user.

Application note 59: The user identified after a successfully performed TA2 is an EAC2 terminal. The types of EAC2 terminals are application dependent;

Application note 60: In the life cycle phase manufacturing, the manufacturer is the only user role known to the TOE. The manufacturer writes the initialization data and/or pre-personalization data in the audit records of the IC.

Note that a personalization agent acts on behalf of the electronic document issuer under his and the CSCA's and DS's policies. Hence, they define authentication procedures for personalization agents. The TOE supports these authentication procedures. These procedures are subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role personalization agent, if a terminal proves the respective Terminal Authorization level (e. g. a privileged terminal, cf. [TR03110-2]).

FIA_UAU.1/PACE_EAC2PP **Timing of authentication**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification

fulfilled by FIA_UID.1/PACE_EAC2PP

FIA_UAU.1.1/PACE_EAC2PP The TSF shall allow

1. to establish a communication channel,
2. carrying out the PACE protocol according to **[TR03110-2]**
3. to read the Initialization Data if it is not disabled by TSF according to ***FMT_MTD.1/INI_DIS_EAC2PP***[155]
4. *none*[156]

on behalf of the user to be performed before the user is authenticated.

[155] [assignment: *list of TSF-mediated actions*]
[156] [assignment: *list of TSF-mediated actions*]

FIA_UAU.1.2/PACE_EAC2PP	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note 61: If PACE has been successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE_EAC2PP. Application note 60 also applies here.

FIA_UAU.1/EAC2_Terminal_EAC2PP **Timing of authentication**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification fulfilled by FIA_UID.1/EAC2_Terminal_EAC2PP

FIA_UAU.1.1/EAC2_Terminal_EAC2PP	The TSF shall allow 1. to establish a communication channel, 2. carrying out the PACE protocol according to [TR03110-2] , 3. to read the Initialization Data if it is not disabled by TSF according to ***FMT_MTD.1/INI_DIS_EAC2PP*** 4. carrying out the Terminal Authentication 2 protocol according to [TR03110-2][157] on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2/EAC2_Terminal_EAC2PP	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note 62: The user authenticated after a successful run of TA2 is an EAC2 terminal. The authenticated terminal will immediately perform Chip Authentication 2 as required by

[157] [assignment: *list of TSF mediated actions*]

FIA_API.1/CA_EAC2PP using, amongst other, Comp(ephem-PK_{PCD}-TA) from the accomplished TA2. Note that Passive Authentication using SOC is considered to be part of CA2 within [EAC2PP].

FIA_UAU.4/PACE_EAC2PP **Single-use authentication of the Terminals by the TOE**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.4.1/PACE_EAC2PP The TSF shall prevent reuse of authentication data related to

1. PACE protocol according to **[TR03110-2]**,
2. Authentication Mechanism based on *AES*[158]
3. Terminal Authentication 2 protocol according to [TR03110-2][159].
4. *none*[160]

Application note 63: For PACE, the TOE randomly selects an almost uniformly distributed nonce of 128 bit length. The current ST supports a key derivation function based on AES; see [TR03110-2]. For TA2, the TOE randomly selects a nonce r_{PICC} of 64 bit length, see [TR03110-2]. This SFR extends FIA_UAU.4/PACE from [PACEPP] by assigning the authentication mechanism Terminal Authentication 2.

FIA_UAU.5/PACE_EAC2PP **Multiple authentication mechanisms**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

[158] [selection: ~~*Triple-DES*~~, *AES or other approved algorithms*]
[159] [assignment: *identified authentication mechanism(s)*]
[160] [assignment: *identified authentication mechanism(s)*]

FIA_UAU.5.1/PACE_EAC2PP

The TSF shall provide

1. PACE protocol according to [**TR03110-2**],
2. Passive Authentication according to [ICAO9303]
3. Secure messaging ~~**in MAC-ENC mode**~~ according to **[TR03110-3]**
4. Symmetric Authentication Mechanism based on *AES*[161]
5. Terminal Authentication 2 protocol according to [TR03110-2],
6. Chip Authentication 2 according to [TR03110-2][162]
7. *none*[163]

to support user authentication.

FIA_UAU.5.2/PACE_EAC2PP

The TSF shall authenticate any user's claimed identity according to the following rules:

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication codes sent by secure messaging with the key agreed with the terminal by the PACE protocol.
2. The TOE accepts the authentication attempt as personalization agent by *the Authentication Mechanism with Personalization Agent Key(s)*[164]
3. The TOE accepts the authentication attempt by means of the Terminal Authentication 2 protocol, only if (i) the terminal presents its static public key PK_{PCD} and the key is successfully verifiable up to the CVCA and (ii) the terminal uses the PICC identifier ID_{PICC} = Comp(ephem-PK_{PICC}-PACE) calculated during, and the secure messaging established by the, current PACE authentication.
4. Having successfully run Chip Authentication 2, the TOE accepts only received commands with correct message authentication codes sent by secure

[161] [selection: *AES or other approved algorithms*]
[162] Passive Authentication using SOC is considered to be part of CA2 within [EAC2PP]
[163] [assignment: *list of multiple authentication mechanisms*]
[164] [selection: *the Authentication Mechanism with Personalization Agent Key(s)*]

messaging with the key agreed with the terminal by Chip Authentication 2[165].

5. *none*[166]

Application note 64: Refinement of FIA_UAU.5.2/PACE_EAC2PP, since here PACE must adhere to [TR03110-2] and [TR03110-3]. Since the formulation "MAC-ENC mode" is slightly ambiguous (there is only one secure messaging mode relevant both in [PACEPP] and here, and it is actually the same in both references), it is removed here by refinement in the third bullet point of FIA_UAU.5.1/PACE_EAC2PP.

Remark: Note that 5. and 6. in FIA_UAU.5.1/PACE_EAC2PP and 3. and 4. of FIA_UAU.5.2/PACE_EAC2PP are additional assignments (using the open assignment operation) compared to [PACEPP].

FIA_UAU.6/CA_EAC2PP **Re-authenticating of Terminal by the TOE**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/CA_EAC2PP The TSF shall re-authenticate the user under the conditions ~~-~~ each command sent to the TOE after a successful run of Chip Authentication 2 shall be verified as being sent by the EAC2 terminal[167].

In addition, this ST includes all remaining SFRs of the claimed [PACEPP]/Class FIA:

FIA_AFL.1/PACE_EAC2PP **Authentication failure handling – PACE authentication using non-blocking authorisation data**

Hierarchical to:

No other components.

[165] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[166] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[167] [assignment: *list of conditions under which re-authentication is required*]

Dependencies:

FIA_UAU.1 Timing of authentication:

fulfilled by FIA_UAU.1/PACE_EAC2PP

FIA_AFL.1.1/PACE_EAC2PP	The TSF shall detect when *10*[168] unsuccessful authentication attempt occurs related to authentication attempts using the PACE password as shared password[169].
FIA_AFL.1.2/PACE_EAC2PP	When the defined number of unsuccessful authentication attempts has been met[170], the TSF shall *increase exponentially the response time*[171].

Application note 65: The open assignment operation shall be performed according to a concrete implementation of the TOE, whereby actions to be executed by the TOE may either be common for all data concerned (PACE passwords, see [ICAO9303]) or for an arbitrary subset of them or may also separately be defined for each datum in question. Since all non-blocking authorisation data (PACE passwords) being used as a shared secret within the PACE protocol do not possess a sufficient entropy[172], the TOE shall not allow a quick monitoring of its behaviour (e.g. due to a long reaction time) in order to make the first step of the skimming attack[173] requiring an attack potential beyond high, so that the threat T.Tracing can be averted in the frame of the security policy of the current ST. One of some opportunities for performing this operation might be 'consecutively increase the reaction time of the TOE to the next authentication attempt using PACE passwords'.

Note here, in addition to the MRZ, the PACE password could also be a CAN or the PIN.

FIA_UAU.6/PACE_EAC2PP **Re-authenticating of Terminal by the TOE**

Hierarchical to:

[168] [assignment: *positive integer number*]
[169] [assignment: *list of authentication events*]
[170] [selection: *met, surpassed*]
[171] [assignment: *list of actions*]
[172] ≥ 100 bits; a theoretical maximum of entropy which can be delivered by a character string is N*ld(C), whereby N is the length of the string, C – the number of different characters which can be used within the string.
[173] guessing CAN or MRZ, see T.Skimming above.

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/PACE_EAC2PP	The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the PACE protocol shall be verified as being sent by the PACE terminal.[174]

Application note 66: The PACE protocol specified in [ICAO9303] starts secure messaging used for all commands exchanged after successful PACE authentication. The TOE checks each command by secure messaging in encrypt-then-authenticate mode based on CMAC or Retail-MAC, whether it was sent by the successfully authenticated terminal (see FCS_COP.1/PACE_MAC_EAC2PP for further details). The TOE does not execute any command with incorrect message authentication code. Therefore, the TOE re-authenticates the terminal connected, if a secure messaging error occurred, and accepts only those commands received from the initially authenticated terminal.

7.1.2.3. SFRs for EAC1-protected data [EAC1PP]

The following SFRs are imported due to claiming [EAC1PP]. They mainly concern authentication mechanisms for applications with EAC1-protected data.

FIA_UAU.1/PACE_EAC1PP	**Timing of authentication**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification fulfilled by FIA_UID.1/PACE_EAC1PP
FIA_UAU.1.1/PACE_EAC1PP	The TSF shall allow 1. to establish the communication channel, 2. carrying out the PACE Protocol according to [ICAO9303], 3. to read the Initialization Data if it is not disabled by TSF according to FMT_MTD.1/INI_DIS_EAC1PP,

[174] [assignment: *list of conditions under which re-authentication is required*]

4. to identify themselves by selection of the authentication key
5. to carry out the Chip Authentication Protocol Version 1 according to [TR03110]
6. to carry out the Terminal Authentication Protocol Version 1 according to [TR03110][175]
7. *none*[176]

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/PACE_EAC1PP The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note 67: The SFR FIA_UAU.1/PACE_EAC1PP in the current ST covers the definition in PACE PP [PACEPP] and extends it by EAC aspect 5. This extension does not conflict with the strict conformance to [PACEPP].

Application note 68: The user authenticated after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device.

If PACE was successfully performed, secure messaging is started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}), cf. FTP_ITC.1/PACE.

FIA_UAU.4/PACE_EAC1PP **Single-use authentication mechanisms - Single-use authentication of the Terminal by the TOE**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.4.1/PACE_EAC1PP The TSF shall prevent reuse of authentication data related to

1. PACE Protocol according to [ICAO9303],

[175] [assignment: *list of TSF-mediated actions*]
[176] [assignment: *list of TSF-mediated actions*]

2. Authentication Mechanism based on *AES*[177]
3. Terminal Authentication Protocol v.1 according to [TR03110][178].

Application note 69: The SFR FIA_UAU.4.1/PACE_EAC1PP in the current ST covers the definition in PACE PP [PACEPP] and extends it by the EAC aspect 3. This extension does not conflict with the strict conformance to [PACEPP]. The generation of random numbers (random nonce) used for the authentication protocol (PACE) and Terminal Authentication as required by FIA_UAU.4/PACE is required by FCS_RND.1 from [PACEPP].

Application note 70: The authentication mechanisms may use either a challenge freshly and randomly generated by the TOE to prevent reuse of a response generated by a terminal in a successful authentication attempt. However, the authentication of Personalisation Agent may rely on other mechanisms ensuring protection against replay attacks, such as the use of an internal counter as a diversifier.

FIA_UAU.5/PACE_EAC1PP **Multiple authentication mechanisms**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UAU.5.1/PACE_EAC1PP The TSF shall provide

1. PACE Protocol according to [ICAO9303],
2. Passive Authentication according to [ICAO9303]
3. Secure messaging in MAC-ENC mode according to [ICAO9303],
4. Symmetric Authentication Mechanism based on *AES*[179]
5. Terminal Authentication Protocol v.1 according to [TR03110],[180]

to support user authentication.

[177] [selection: *Triple-DES, AES or other approved algorithms*]
[178] [assignment: *identified authentication mechanism(s)*]
[179] [selection: *Triple-DES, AES or other approved algorithms*]
[180] [assignment: *list of multiple authentication mechanisms*]

FIA_UAU.5.2/PACE_EAC1PP The TSF shall authenticate any user's claimed identity according to the following rules:

1. Having successfully run the PACE protocol the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with the key agreed with the terminal by means of the PACE protocol.
2. The TOE accepts the authentication attempt as Personalisation Agent by *the Authentication Mechanism with Personalisation Agent Key(s)*[181].
3. After run of the Chip Authentication Protocol Version 1 the TOE accepts only received commands with correct message authentication code sent by means of secure messaging with key agreed with the terminal by means of the Chip Authentication Mechanism v1.
4. The TOE accepts the authentication attempt by means of the Terminal Authentication Protocol v.1 only if the terminal uses the public key presented during the Chip Authentication Protocol v.1 and the secure messaging established by the Chip Authentication Mechanism v.1[182].
5. *none*[183].

Application note 71: The SFR FIA_UAU.5.1/PACE_EAC1 covers the definition in [PACEPP] and extends it by EAC aspects 4), 5), and 6). The SFR FIA_UAU.5.2/PACE_EAC1 covers the definition in [PACEPP] and extends it by EAC aspects 2), 3), 4) and 5). These extensions do not conflict with the strict conformance to [PACEPP].

FIA_UAU.6/PACE_EAC1PP **Re-authenticating of Terminal by the TOE**

(equivalent to FIA_UAU.6/PACE_EAC2PP, but listed here for the sake of completeness)

FIA_UAU.6/EAC_EAC1PP **Re-authenticating – Re-authenticating of Terminal by the TOE**

Hierarchical to:

[181] [selection: *the Authentication Mechanism with Personalisation Agent Key(s)*]
[182] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]
[183] [assignment: *rules describing how the multiple authentication mechanisms provide authentication*]

No other components.

Dependencies:

No dependencies.

FIA_UAU.6.1/EAC_EAC1PP The TSF shall re-authenticate the user under the conditions each command sent to the TOE after successful run of the Chip Authentication Protocol Version 1 shall be verified as being sent by the Inspection System.[184]

Application note 72: The Password Authenticated Connection Establishment and the Chip Authentication Protocol specified in [ICAO9303] include secure messaging for all commands exchanged after successful authentication of the Inspection System. The TOE checks by secure messaging in MAC_ENC mode each command based on a corresponding MAC algorithm whether it was sent by the successfully authenticated terminal (see FCS_COP.1/CA_MAC_EAC1PP for further details). The TOE does not execute any command with incorrect message authentication code. Therefore the TOE re-authenticates the user for each received command and accepts only those commands received from the previously authenticated user.

FIA_API.1/EAC1PP Authentication Proof of Identity

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_API.1.1/EAC1PP The TSF shall provide a Chip Authentication Protocol Version 1 according to [TR03110][185] to prove the identity of the TOE[186].

Application note 73: This SFR requires the TOE to implement the Chip Authentication Mechanism v.1 specified in [TR03110]. The TOE and the terminal generate a shared secret using the Diffie-Hellman Protocol (EC-DH) and two session keys for secure messaging in ENC_MAC mode according to [ICAO9303]. The terminal verifies by means of secure messaging

[184] [assignment: *list of conditions under which re-authentication is required*]
[185] [assignment: *authentication mechanism*]
[186] [assignment: *authorized user or role*]

whether the travel document's chip was able or not to run his protocol properly using its Chip Authentication Private Key corresponding to the Chip Authentication Key (EF.DG14).

FIA_AFL.1/PACE_EAC1PP **Authentication failure handling – PACE authentication using non-blocking authorisation data**

(equivalent to FIA_AFL.1/PACE_EAC2PP, but listed here for the sake of completeness)

FIA_UID.1/PACE_EAC1PP **Timing of identification**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FIA_UID.1.1/PACE_EAC1PP The TSF shall allow

1. to establish the communication channel,
2. carrying out the PACE Protocol according to [ICAO9303],
3. to read the Initialization Data if it is not disabled by TSF according to *FMT_MTD.1/INI_DIS_EAC1PP*,
4. to carry out either the Chip Authentication Protocol v.1 according to [TR03110-1],
5. to carry out the Terminal Authentication Protocol v.1 according to [TR03110-1]
6. *none*[187]

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/PACE_EAC1PP The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note 74: The SFR FIA_UID.1/PACE_EAC1PP in the current ST covers the definition in [PACEPP] and extends it by EAC aspect 4. This extension does not conflict with the strict conformance to [PACEPP].

Application note 75: In the Phase 2 "Manufacturing of the TOE" the Manufacturer is the only user role known to the TOE which writes the Initialization Data and/or Pre-personalisation

[187] [assignment: *list of TSF-mediated actions*]

Data in the audit records of the IC. The travel document manufacturer may create the user role Personalisation Agent for transition from Phase 2 to Phase 3 “Personalisation of the travel document”. The users in role Personalisation Agent identify themselves by means of selecting the authentication key. After personalisation in the Phase 3 the PACE domain parameters, the Chip Authentication data and Terminal Authentication Reference Data are written into the TOE. The Inspection System is identified as default user after power up or reset of the TOE i.e. the TOE will run the PACE protocol, to gain access to the Chip Authentication Reference Data and to run the Chip Authentication Protocol Version 1. After successful authentication of the chip the terminal may identify itself as (i) Extended Inspection System by selection of the templates for the Terminal Authentication Protocol Version 1 or (ii) if necessary and available by authentication as Personalisation Agent (using the Personalisation Agent Key).

Application note 76: User identified after a successfully performed PACE protocol is a terminal. Please note that neither CAN nor MRZ effectively represent secrets, but are restricted revealable; i.e. it is either the travel document holder itself or an authorised other person or device (Basic Inspection System with PACE).

Application note 77: In the life-cycle phase ‘Manufacturing’ the Manufacturer is the only user role known to the TOE. The Manufacturer writes the Initialisation Data and/or Pre-personalisation Data in the audit records of the IC.Please note that a Personalisation Agent acts on behalf of the travel document Issuer under his and CSCA and DS policies. Hence, they define authentication procedure(s) for Personalisation Agents. The TOE must functionally support these authentication procedures being subject to evaluation within the assurance components ALC_DEL.1 and AGD_PRE.1. The TOE assumes the user role ‘Personalisation Agent’, when a terminal proves the respective Terminal Authorisation Level as defined by the related policy (policies).

7.1.2.4. SFRs concerning eSign-applications [SSCDPP]

The following SFRs are imported due to claiming [SSCDPP]. They concern access mechanisms for an eSign application.

FIA_UID.1/SSCDPP	**Timing of identification**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1/SSCDPP	The TSF shall allow (1) Self-test according to FPT_TST.1/SSCDPP,

(2) *To establish a trusted channel between the user and the TOE and to establish a trusted channel between the SCA and the TOE*[188],

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/SSCDPP — The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1/SSCDPP — **Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

fulfilled by FIA_UAU.1/SSCDPP

FIA_AFL.1.1/SSCDPP — The TSF shall detect when *3*[189] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[190].

FIA_AFL.1.2/SSCDPP — When the defined number of unsuccessful authentication attempts has been met[191], the TSF shall block RAD[192].

FIA_AFL.1/BIO_SSCDPP — **Authentication failure handling**

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

fulfilled by FIA_UAU.1/SSCDPP

[188] [assignment: *list of additional TSF-mediated actions*]
[189] [selection: [assignment: *positive integer number], an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
[190] [assignment: *list of authentication events*]
[191] [selection: *met ,surpassed*]
[192] [assignment: *list of actions*]

FIA_AFL.1.1/BIO_SSCDPP	The TSF shall detect when 24[193] unsuccessful authentication attempts occur related to consecutive failed authentication attempts[194].
FIA_AFL.1.2/BIO_SSCDPP	When the defined number of unsuccessful authentication attempts has been met[195], the TSF shall block RAD[196].

FIA_API.1/SSCDPP4	**Authentication Proof of Identity**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_API.1.1/SSCDPP4	The TSF shall provide an *administrator secure channel*[197] to prove the identity of the *SSCD*[198].

The next claimed SFR is refined from [SSCDPP], [SSCDPP4] and [SSCDPP5] by additional assignments. Note that this does not violate strict conformance to [SSCDPP].

FIA_UAU.1/SSCDPP **Timing of authentication**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification:

fulfilled by FIA_UID.1/SSCDPP

FIA_UAU.1.1/SSCDPP

The TSF shall allow

1. self test according to ***FPT_TST.1/SSCDPP***,

[193] [selection: [assignment: *positive integer number], an administrator configurable positive integer within* [assignment: *range of acceptable values*]]
[194] [assignment: *list of authentication events*]
[195] [selection: *met ,surpassed*]
[196] [assignment: *list of actions*]
[197] [assignment: *authentication mechanism*]
[198] [assignment: *authorized user or rule*]

2. identification of the user by means of TSF required by FIA_UID.1/SSCDPP,
3. *establishing a trusted channel between CGA and the TOE by means of TSF required by FTP_ITC.1/SVD_SSCDPP4 and FTP_ITC.1/CA_EAC2PP respectively,*
4. *establishing a trusted channel between HID and the TOE by means of TSF required by FTP_ITC.1/VAD_SSCDPP5 and FTP_ITC.1/CA_EAC2PP respectively,*
5. *none*[199].

on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/SSCDPP

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.3. Class FDP

7.1.3.1. SFRs for from [MR.ED-PP]

Multiple iterations of FDP_ACF.1 exist from imported PPs to define the access control SFPs for (common) user data, EAC1-protected user data, and EAC2-protected user data. The access control SFPs defined in FDP_ACF.1/EAC1PP from [EAC1PP] and FDP_ACF.1/EAC2PP from [EAC2PP] are here unified to one single FDP_ACF.1/TRM, whereas the several iterations of FDP_ACF.1 from [SSCDPP] stand separate. Here we take FDP_ACF.1/EAC2PP as a base definition of functional elements, and it is refined in a way that it is compatible with FDP_ACF.1/EAC1PP. Hence highlighting refers to changes w.r.t. to FDP_ACF.1/EAC2PP. In the application note below, we explain how FDP_ACF.1/EAC1PP is covered as well.

Concerning FDP_ACF.1/TRM here and the several iterations FDP_ACF.1 from [SSCDPP], we remark that FDP_ACF.1/TRM also concerns data and objects for signature generation. Note however, that FDP_ACF.1/TRM requires that prior to granting access to the signature application, in which the access controls defined in [SSCDPP] apply, an EAC2 terminal and the electronic document holder need to be authenticated. Hence, no inconsistency exist.

FDP_ACF.1/TRM Security attribute based access control – Terminal Access

Hierarchical to:

No other components.

Dependencies:

FDP_ACC.1 Subset access control

[199] [assignment: *list of additional TSF-mediated actions*]

fulfilled by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP

FMT_MSA.3 Static attribute initialization

not fulfilled, but **justified**:

The access control TSF according to FDP_ACF.1/TRM uses security attributes having been defined during the personalization and fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1/Admin_SSCDPP, FMT_MSA.1/Signatory_SSCDPP and FMT_MSA.3/SSCDPP) is necessary here.

FDP_ACF.1.1/TRM The TSF shall enforce the *Access Control SFP*[200] to objects based on the following:

1) *Subjects:*
   a) *Terminal,*
   b) *PACE terminal ,*
   c) *EAC2 terminal Inspection system, authentication terminal, signature terminal,*
   d) *EAC1 terminal*[201]*;*
2) *Objects:*
   a) *all user data stored in the TOE; including sensitive EAC1-protected user data, and sensitive EAC2-protected user data.*
   b) *all TOE intrinsic secret (cryptographic) data*
3) *Security attributes:*
   a) *Terminal Authorization Level (access rights)*
   b) *Authentication status of the electronic document holder as a signatory (as an eSign application is included)*[202] [203].

FDP_ACF.1.2/TRM The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

A PACE terminal is allowed to read data objects from FDP_ACF.1/TRM after successful PACE authentication according to [TR03110-2] **and/or [ICAO9303]**, as required by FIA_UA*U.1/PACE.*[204]

[200] [assignment: *access control SFP*]
[201] [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [EAC2PP]*)
[202] [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (added using open assignment of [EAC2PP]*)
[203] [assignment: *list of subjects and objects controlled under the indicated SFP, and, for each, the SFP-relevant security attributes, or name groups of SFP-relevant security attributes] (all bullets in FDP_ACF.1.1/TRM w.r.t. CC part 2 [CC]*)

FDP_ACF.1.3/TRM The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none.*[205]

FDP_ACF.1.4/TRM The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

1. *Any terminal not being a PACE terminal or an EAC2 terminal or an EAC1 terminal is not allowed to read, to write, to modify, or to use any user data stored on the electronic document.*[206]
2. *Terminals not using secure messaging are not allowed to read, write, modify, or use any data stored on the electronic document.*
3. *No subject is allowed to read 'Communication Establishment Authorization Data' stored on the electronic document*
4. *No subject is allowed to write or modify 'secret electronic document holder authentication data' stored on the electronic document, except for PACE terminals or EAC2 terminals executing PIN management based on the following rules:*
   Change PIN, Resume PIN, Resume PUK, Unblock PIN, Activate PIN, Deactivate PIN.
5. *No subject is allowed to read, write, modify, or use ~~the private Restricted Identification key(s)~~ and Chip Authentication key(s) stored on the electronic document.*
6. *Reading, modifying, writing, or using sensitive user data that are protected only by EAC2, is allowed only to EAC2 terminals using the following mechanism:*
   The TOE applies the EAC2 protocol (cf. FIA_UAU.5) to determine access rights of the terminal according to [TR03110-2]. To determine the effective authorization of a terminal, the chip must calculate a bitwise Boolean 'and' of the relative authorization contained in the CHAT of the Terminal Certificate, the referenced DV Certificate, and the referenced CVCA Certificate, and additionally the confined authorization sent as part of PACE. Based on that effective authorization and the terminal type drawn from the CHAT of the Terminal Certificate, the TOE shall grant the right to read, modify or write sensitive user data, or perform operations using these sensitive user data.
7. *No subject is allowed to read, write, modify or use the data objects 2b) of FDP_ACF.1.1/TRM.*

---

[204] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[205] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[206] note that authentication of an EAC1 or EAC2 terminal to a TOE in certified mode implies a prior run of PACE.

8. *No subject is allowed to read sensitive user data that are protected only by EAC1, except an EAC1 terminal (OID inspection system) after EAC1, cf. FIA_UAU.1/EAC1, that has a corresponding relative authorization level. This includes in particular EAC1-protected user data DG3 and DG4 from an ICAO-compliant ePass application, cf. [TR03110-1] and [ICAO9303] .*
9. *If sensitive user data is protected both by EAC1 and EAC2, no subject is allowed to read those data except EAC1 terminals or EAC2 terminals that access these data according to rule 6 or rule 8 above.*
10. *Nobody is allowed to read the private signature key(s).*[207]

Application note 78: The above definition is based on FDP_ACF.1/TRM_EAC2PP. We argue that it covers FDP_ACF.1/TRM_EAC1PP as well. Subject 1b and 1d are renamed here from FDP_ACF.1.1/TRM_EAC1PP according to **Tabla 1**. Objects in 2), in particular the term EAC1-protected user data, subsume all those explicitly enumerated in FDP_ACF.1.1/TRM_EAC1PP. Also the security attribute 3a) Terminal Authorization Level here subsumes the explicitly enumerated attributes 3a) and 3b) of FDP_ACF.1.1/TRM_EAC1PP, but are semantically the same. Since in addition EAC2 protected data are stored in the TOE of this ST, additional subjects, objects and security attributes are listed here. However since they apply to data with a different protection mechanism (EAC2), strict conformance is not violated.

FDP_ACF.1.2/TRM uses the renaming of **Tabla 1**, and references in addition [TR03110-2]. However the references are compatible as justified in [EAC2PP], yet both are mentioned here since [TR03110-2] is the primary norm for an eID application, whereas [ICAO9303] is normative for an ICAO compliant ePass application. Investigating the references reveals that access to data objects defined in FDP_ACF.1.1/TRM must be granted if these data are neither EAC1-protected, nor EAC2-protected.

FDP_ACF.1.3/TRM is the same as in FDP_ACF.1.3/TRM_EAC2PP.

References are changed in FDP_ACF.1.2/TRM_EAC1PP. It is already justified in [EAC2PP] that definitions in [TR03110-2] and [ICAO9303] are compatible.

FDP_ACF.1.3/TRM is taken over from [EAC1PP] and [EAC2PP] (same formulation in both).

Rules 1 and 2 of FDP_ACF.1.4/TRM_EAC1PP in [EAC1PP] are covered by their counterparts rule 1 and rule 2 here. Rules 3 and 4, and rule 6 of FDP_ACF.1.4/TRM_EAC1PP in [EAC1PP] are combined here to rule 8, where terminals need the corresponding CHAT to read data groups. Rule 5 of [EAC1PP] is here equivalent to rule 7. None of this conflicts with strict conformance to [EAC1PP]. Note that adding additional rules compared to FDP_ACF.1.4/TRM_EAC1PP here can never violate strict conformance, as these are rules that explicitly deny access of subjects to objects. Hence security is always increased.

[207] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

The above definition also covers FDP_ACF.1.1/TRM_EAC2PP and extends it by additional subjects and objects. Sensitive user data in the definition of FDP_ACF.1.1/TRM_EAC2PP are here EAC2-protected sensitive user data. EAC1-protected data are added here by refinement. Since the protection level and mechanisms w.r.t. to EAC2-protected data do not change, strict conformance is not violated.

FDP_ACF.1.2/TRM_EAC2PP and FDP_ACF.1.3/TRM_EAC2PP are equivalent to the current definition. Rules 8, 9 and 10 are added here by open assignment from [EAC2PP]. None of this conflicts with strict conformance.

The dependency of this SFR is met by FDP_ACC.1/TRM_EAC1PP and FDP_ACC.1/TRM_EAC2PP. Note that the SFR in [EAC1PP] applies the assignment operation, whereas in [EAC2PP] (by referencing [PACEPP]) the assignment is left open. Hence they are compatible. We remark that in order to restrict the access to user data as defined in the SFR FDP_ACC.1/TRM_EAC1PP, clearly access to objects 2b) of FDP_ACF.1.1/TRM must be restricted as well according to the SFP, otherwise access to user data is impossible to enforce.

7.1.3.2. SFRs for [MR.ED-ON-PP]

FDP_ACC.1/UPD **Subset Access Control – Terminal Access**

Hierarchical to:

No other components.

Dependencies:

FDP_ACF.1 Security attribute based access control:

fulfilled by FDP_ACF.1/UPD

FDP_ACC.1.1/UPD The TSF shall enforce the *Update Access Control SFP*[208] on

1) *Subjects:*
   a) *terminal,*
   b) *update terminal.*
2) *Objects:*
   a) *version information identifying the TOE software*
   b) *update package*
   c) *update log information*
3) *Operations:*

[208] [assignment: *access control SFP*]

a) *reading out version information*,
b) *reading out log data*,
c) *uploading an update package on the TOE, or*
d) *initiating an update procedure*

and *none*[209].

FDP_ACF.1/UPD **Security Attribute based Access Control – Terminal Access**

Hierarchical to:

No other components.

Dependencies:

FDP_ACC.1 Subset access control

fulfilled by FDP_ACC.1/UPD

FMT_MSA.3 Static attribute initialization

not fulfilled, but **justified**:

The access control TSF according to FDP_ACF.1/UPD uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1/Admin_SSCDPP, FMT_MSA.1/Signatory_SSCDPP and FMT_MSA.3/SSCDPP) is necessary here.

FDP_ACF.1.1/UPD The TSF shall enforce the *Update Access Control SFP*[210] to objects based on the following:

1) *Subjects:*
   a) *terminal*,
   b) *update terminal*
2) *Objects:*
   a) *version information identifying the TOE software*
   b) *update package*
   c) *update log information*
3) *Security attributes:*
   a) *access rights*
4) *none*[211].

[209] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[210] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]]

FDP_ACF.1.2/UPD

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

The authentication level of a terminal must be determined by a successful establishment of a secure channel according to[EN419212-3] as required by FIA_UAU.1/UPD. Depending on the authentication level, an authenticated update terminal is allowed one ~~or more~~ of the following:

- ~~*read one or more data objects from FDP_ACF.1/UPD*~~
- ~~*upload an update package to the TOE and*~~ *initiate the update procedure.*

The precise definition of access rights and how the authentication level is calculated from an authenticated terminal is defined in [GOA].

Once the terminal is authenticated to initiate the update procedure, it must establish a secure channel using the session keys from FCS_CKM.1.1/UPD_INT and FCS_CKM.1.1/UPD_DEC to be authenticated to the loader as required by FIA_UAU.1/UPD; then, the terminal can start to upload each update package ensuring its integrity and confidentiality[212].

FDP_ACF.1.3/UPD

The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: *none*.[213]

FDP_ACF.1.4/UPD

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: *none.*[214]

FDP_IFC.1/UPD **Subset information flow control**

[211] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[212] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[213] [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*]
[214] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

Hierarchical to:

No other components.

Dependencies:

FDP_IFF.1 Simple security attributes,

fulfilled by FDP_IFF.1/UPD

FDP_IFC.1.1/UPD The TSF shall enforce the *Update Flow Control SFP*[215] on *the following*:

1) *Subjects:*
   a) *terminal,*
   b) *update terminal.*
2) *information:*
   a) *update package*
   b) *update data*
   c) *c)meta-data, such as version information*
3) *operations:*
   a) *performing an update*[216].

FDP_IFF.1/UPD Simple Security Attributes

Hierarchical to:

No other components.

Dependencies:

FDP_IFC.1 Subset information flow control:

fulfilled by FDP_IFC.1/UPD

FMT_MSA.3 Static attribute initialization:

not fulfilled, but **justified**:

The update control TSF according to FDP_IFF.1/UPD uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1/Admin_SSCD y FMT_MSA.1/Signatory_SSCDPP and FMT_MSA.3/SSCDPP) is necessary here.

[215] [assignment: *information flow control SFP*]
[216] [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*]

FDP_IFF.1.1/UPD

The TSF shall enforce the *Update Control SFP*[217] based on the following types of subject and information security attributes:

1) *Subjects:*
   a) *terminal,*
   b) *update terminal.*
2) *information:*
   a) *update package*
   b) *update data*
   c) *meta-data, such as version information*
3) *security attributes:*
   a) *update package verification status with the values: NOT VERIFIED (default status), SUCCESSFULLY VERIFIED, and VERIFICATION FAILED*[218].

FDP_IFF.1.2/UPD

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

1. *The terminal has established a secure channel with the TOE.*
2. *The TOE shall only accept update packages sent via a secure channel established with an authenticated update terminal*[219].

FDP_IFF.1.3/UPD

The TSF shall enforce the *following rules in their specific order:*

1) The authenticity (using the digital signature, cf. FCS_COP.1/UPD_SIG) of the first step of the updating process is verified by the OS. If the authenticity is not validated, abort with VERIFICATION FAILED. If the OS identifier is not verified as correct according to [none] the security attribute is set to VERIFICATION FAILED.

2) ***Once the OS has verified the authenticity correctly, the update package process starts using the loader mechanism.*** *The integrity (using the keyed or unkeyed hash function cf. FCS_COP.1/UPD_INT) ~~and authenticity (using the digital signature, cf. FCS_COP.1/UPD_SIG) of the first part~~ of the update package is verified. If the integrity ~~and~~*

[217] [assignment: *information flow control SFP*]
[218] [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*]
[219] [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*]

~~authenticity are~~ is not ~~both~~ validated, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1/UPD.

3) *The ~~first part of the~~ update package is only decrypted, cf. FCS_COP.1/UPD_DEC, if the integrity ~~and authenticity of the that part~~ has been verified in rule **2**. If the decryption fails, abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1/UPD.*
4) *~~If all parts of the update package have been decrypted, continue with rule 4. Otherwise, apply rules 1. and 2. on the remaining parts (replace 'first part' with 'current part' above) until either all parts have been decrypted, or the procedure has been aborted with VERIFICATION FAILED.~~ For each update package, steps 2 and 3 will be repeated.*
5) *~~If additional meta-data is stored in the update package version, OS identifier is not verified as correct according to [GOA] the security attribute is set to VERIFICATION FAILED and the update package including all associated data are destroyed, cf. FDP_RIP.1/UPD. Correctness w.r.t. the referenced technical specification must not contradict any of the given rules here.~~*
6) *~~Next, the TSF shall verify that:~~*
    a) *~~the version number of the update package must be greater than the version of the installed corresponding software package;~~*
    b) *~~the update data are suitable to the specific TOE configuration/platform by checking relevant meta-data (i.e. TOE product identifier, version number etc.).~~*

If all conditions ~~in step 5~~ are verified, the verification status is set to SUCCESSFULLY VERIFIED. Otherwise abort with VERIFICATION FAILED, and erase all data transferred so far, cf. FDP_RIP.1/UPD.

Only if the verification status is SUCCESSFULLY VERIFIED, the TOE shall install the update data[220].

FDP_IFF.1.4/UPD	The TSF shall explicitly authorize an information flow based on the following rules: *none*[221].

[220] [assignment: *additional information flow control SFP rules*]
[221] [assignment: *rules, based on security attributes, that explicitly authorize information flows*]

FDP_IFF.1.5/UPD The TSF shall explicitly deny an information flow based on the following rules: *none*[222].

FDP_RIP.1/UPD Subset Residual Information Protection

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_RIP.1.1/UPD The TSF shall ensure that any previous information content of a resource is made unavailable upon *the deallocation of the resource from*[223] the following objects:

1) *session keys (immediately after closing related communication session),*
2) *all ephemeral keys related to the update mechanism.*
3) *Update package, decrypted update data and meta-data uploaded to the TOE or generated during the update procedure*
4) *none*[224].

Application note 79: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1/UPD requires a certain quality metric ('any previous information content of a resource is made unavailable') for key destruction in addition to FCS_CKM.4 that merely requires a fact of key destruction according to a method/standard. The update procedure is defined in [GOA].

7.1.3.3. SFRs for [EAC2PP]

The following SFRs are imported due to claiming [EAC2PP]. They concern access control mechanisms related to EAC2-protected data.

FDP_ACC.1/TRM_EAC2PP Subset access control – Terminal Access

[222] [assignment: *rules, based on security attributes, that explicitly deny information flows*]
[223] [selection: *allocation of the resource to, deallocation of the resource from*]
[224] [assignment: *list of objects*]

Hierarchical to:

No other components.

Dependencies:

FDP_ACF.1 Security attribute based access control:

fulfilled by FDP_ACF.1/TRM

FDP_ACC.1.1/TRM_EAC2PP The TSF shall enforce the Access Control SFP[225] on terminals gaining access to the User Data and data stored in EF.SOD of the electronic document.[226] and *none*[227].

Application note 80: The Protection Profile [PACEPP] allows for extension to cover additional security functionalities. This is not necessary here, as all security functionalities are covered by FDP_ACF.1/TRM_EAC2PP.

Application note 81: Note that "user data" as defined in FDP_ACC.1/TRM_EAC2PP here includes both common and sensitive user data. For the access control SFP, see FDP_ACF.1/TRM_EAC2PP.

This SFR is equivalent to/covered by FDP_ACC.1/TRM_EAC1PP; cf. the application note above.

FDP_ACF.1/TRM_EAC2PP Security attribute based access control – Terminal Access

This SFR is equivalent to/covered by FDP_ACF.1/TRM.

FDP_RIP.1/EAC2PP Subset residual information protection

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FDP_RIP.1.1/EAC2PP The TSF shall ensure that any previous information content of a resource is made unavailable upon the *deallocation of the resource from*[228] the following objects:

[225] [assignment: *access control SFP*]
[226] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[227] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

1. Session keys (**PACE-K_{MAC}, PACE-K_{Enc}**), (**CA-K_{MAC}, CA-K_{Enc}**) (immediately after closing related communication session),
2. the ephemeral private key ephem - SK_{PICC}- PACE (by having generated a DH shared secret K),
3. secret electronic document holder authentication data, e.g. PIN and/or PUK (when their temporarily stored values are not used any more)
4. *none*[229],

Application note 82: The functional family FDP_RIP possesses such a general character, that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-Data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1/EAC2PP requires a certain quality metric (any previous information content of a resource is made unavailable) for key destruction in addition to FCS_CKM.4/PACEPP that merely requires to ensure key destruction according to a method/standard.

Application note 83: This SFR covers also FDP_RIP.1/EAC1PP from the [EAC1PP].

FDP_UCT.1/TRM_EAC2PP Basic data exchange confidentiality – MRTD

Hierarchical to:

No other components.

Dependencies:

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

fulfilled by FTP_ITC.1/PACE_EAC2PP

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

fulfilled by FDP_ACC.1/TRM_EAC2PP

FDP_UCT.1.1/TRM_EAC2PP The TSF shall enforce the Access Control SFP[230] to be able to transmit and receive[231] user data in a manner protected from unauthorised disclosure.

[228] [selection: *allocation of the resource to, deallocation of the resource from*]
[229] [assignment: *list of objects*]
[230] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]

FDP_UIT.1/TRM_EAC2PP Data exchange integrity

Hierarchical to:

No other components.

Dependencies:

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

fulfilled by FTP_ITC.1/PACE_EAC2PP

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

fulfilled by FDP_ACC.1/TRM_EAC2PP

FDP_UIT.1.1/TRM_EAC2PP The TSF shall enforce the Access Control SFP[232] to be able to transmit and receive[233] user data in a manner protected from modification, deletion, insertion and replay[234] errors.

FDP_UIT.1.2/TRM_EAC2PP The TSF shall be able to determine on receipt of user data, whether modification, deletion, insertion and replay[235] has occurred.

7.1.3.4. SFRs for [EAC1PP]

The following SFRs are imported due to claiming [EAC1PP]. They concern access control mechanisms related to EAC1-protected data.

FDP_ACC.1/TRM_EAC1PP Subset access control

The SFR is equivalent to FDP_ACC.1/TRM_EAC2PP, since EF.SOD (cf. FDP_ACC.1/TRM in [EAC1PP]) can be considered user data.; cf. also the application note below FDP_ACF.1/TRM_EAC1PP.

---

[231] [selection: *transmit, receive*]
[232] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[233] [selection: *transmit, receive*]
[234] [selection: *modification, deletion, insertion, replay*]
[235] [selection: *modification, deletion, insertion, replay*]

FDP_ACF.1/TRM_EAC1PP Security attribute based access control

This SFR is equivalent to/covered by FDP_ACF.1/TRM_EAC2PP.

FDP_RIP.1/EAC1PP Subset residual information protection

This SFR is equivalent to/covered by FDP_RIP.1/EAC2PP.

Application note 84: The functional family FDP_RIP possesses such a general character, so that it is applicable not only to user data (as assumed by the class FDP), but also to TSF-data; in this respect it is similar to the functional family FPT_EMS. Applied to cryptographic keys, FDP_RIP.1/EAC1PP requires a certain quality metric ('any previous information content of a resource is made unavailable') for key's destruction in addition to FCS_CKM.4/PACEPP that merely requires a fact of key destruction according to a method/standard.

FDP_UCT.1/TRM_EAC1PP Basic data exchange confidentiality – MRTD

(equivalent to FDP_UCT.1/TRM_EAC2PP, but listed here for the sake of completeness)

FDP_UIT.1/TRM_EAC1PP Data exchange integrity

(equivalent to FDP_UIT.1/TRM_EAC2PP, but listed here for the sake of completeness)

7.1.3.5. SFRs for [SSCDPP]

The following SFRs are imported due to claiming [SSCDPP]. They concern access control mechanisms of an *eSign* application.

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised

SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)

FDP_ACC.1/SCD/SVD_Generation_SSCDPP Subset access control

Hierarchical to:

No other components.

Dependencies:

FDP_ACF.1 Security attribute based access control

fulfilled by FDP_ACF.1/SCD/SVD_Generation_SSCDPP

FDP_ACC.1.1/SCD/SVD_Generation_SSCDPP The TSF shall enforce the SCD/SVD Generation SFP[236] on

(1) subjects: S.User,

(2) objects: SCD, SVD,

(3) operations: generation of SCD/SVD pair[237].

FDP_ACF.1/SCD/SVD_Generation_SSCDPP Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

fulfilled by FDP_ACC.1/SCD/SVD_Generation_SSCDPP

FMT_MSA.3 Static attribute initialization

fulfilled by FMT_MSA.3/SSCDPP

[236] [assignment: *access control SFP*]
[237] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]

FDP_ACF.1.1/SCD/SVD_Generation_SSCDPP	The TSF shall enforce the SCD/SVD Generation SFP[238] to objects based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[239].
FDP_ACF.1.2/SCD/SVD_Generation_SSCDPP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to generate SCD/SVD pair[240].
FDP_ACF.1.3/SCD/SVD_Generation_SSCDPP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[241].
FDP_ACF.1.4/SCD/SVD_Generation_SSCDPP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair[242].

FDP_ACC.1/SVD_Transfer_SSCDPP **Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

fulfilled by FDP_ACF.1/SVD_Transfer_SSCDPP

FDP_ACC.1.1/SVD_Transfer_SSCDPP	The TSF shall enforce the SVD Transfer SFP[243] on (1) subjects: S.User,

[238] [assignment: *access control SFP*]
[239] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[240] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[241] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[242] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[243] [assignment: *access control SFP*]

(2) objects: SVD

(3) operations: export[244].

FDP_ACF.1/SVD_Transfer_SSCDPP	**Security attribute based access control**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control fulfilled by FDP_ACC.1/SVD_Transfer_SSCDPP FMT_MSA.3 Static attribute initialisation fulfilled by FMT_MSA.3/SSCDPP

FDP_ACF.1.1/SVD_Transfer_SSCDPP	The TSF shall enforce the SVD Transfer SFP[245] to objects based on the following: (1) the S.User is associated with the security attribute Role, (2) the SVD[246].
FDP_ACF.1.2/SVD_Transfer_SSCDPP	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: *R.Admin, R.Sigy* is allowed to export SVD[247].
FDP_ACF.1.3/SVD_Transfer_SSCDPP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[248].
FDP_ACF.1.4/SVD_Transfer_SSCDPP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[249].

[244] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[245] [assignment: *access control SFP*]
[246] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]
[247] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]]
[248] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[249] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]

FDP_ACC.1/Signature-creation_SSCDPP **Subset access control**

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

fulfilled by FDP_ACF.1/Signature-creation_SSCDPP

FDP_ACC.1.1/Signature_Creation_SSCDPP The TSF shall enforce the Signature Creation SFP[250] on

(1) subjects: S.User,

(2) objects: DTBS/R, SCD,

(3) operations: signature creation[251].

FDP_ACF.1/Signature-creation_SSCDPP **Security attribute based access control**

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

fulfilled by FDP_ACC.1/Signature-creation_SSCDPP

FMT_MSA.3 Static attribute initialisation

fulfilled by FMT_MSA.3/SSCDPP

FDP_ACF.1.1/Signature_Creation_SSCDPP The TSF shall enforce the Signature Creation SFP[252] to objects based on the following:

(1) the user S.User is associated with the security attribute "Role" and

(2) the SCD with the security attribute "SCD Operational"[253].

FDP_ACF.1.2/Signature_Creation_SSCDPP The TSF shall enforce the following rules to determine if an operation among

[250] [assignment: *access control SFP*]
[251] [assignment: *list of subjects, objects, and operations among subjects and objects covered by the SFP*]
[252] [assignment: *access control SFP*]
[253] [assignment: *list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes*]

	controlled subjects and controlled objects is allowed: R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"[254].
FDP_ACF.1.3/Signature_Creation_SSCDPP	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[255].
FDP_ACF.1.4/Signature_Creation_SSCDPP	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"[256].

FDP_RIP.1/SSCDPP	**Subset residual information protection**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FDP_RIP.1.1/SSCDPP	The TSF shall ensure that any previous information content of a resource is made unavailable upon the de-allocation of the resource from[257] the following objects: SCD[258].

The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":

1. SCD
2. SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

[254] [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*]
[255] [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*]
[256] [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*]
[257] [selection: *allocation of the resource to, deallocation of the resource from*]
[258] [assignment: *list of objects*]

FDP_SDI.2/Persistent_SSCDPP	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
FDP_SDI.2.1/Persistent_SSCDPP	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[259] on all objects, based on the following attributes: integrity checked stored data[260].
FDP_SDI.2.2/Persistent_SSCDPP	Upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data (2) inform the S.Sigy about integrity error[261].

FDP_SDI.2/DTBS_SSCDPP	**Stored data integrity monitoring and action**
Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.
FDP_SDI.2.1/DTBS_SSCDPP	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[262] on all objects, based on the following attributes: integrity checked stored DTBS[263].
FDP_SDI.2.2/DTBS_SSCDPP	Upon detection of a data integrity error, the TSF shall (1) prohibit the use of the altered data (2) inform the S.Sigy about integrity error[264].

7.1.3.6. SFRs for [SSCDPP4]

FDP_DAU.2/SVD_SSCDPP4	**Data Authentication with Identity of Guarantor**
Hierarchical to:	FDP_DAU.1 Basic Data Authentication
Dependencies:	FIA_UID.1 Timing of identification fulfilled by FIA_UID.1/SSCDPP

[259] [assignment: *integrity errors*]
[260] [assignment: *user data attributes*]
[261] [assignment: *action to be taken*]
[262] [assignment: *integrity errors*]
[263] [assignment: *user data attributes*]
[264] [assignment: *action to be taken*]

FDP_DAU.2.1/SVD_SSCDPP4	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of SVD[265].
FDP_DAU.2.2/SVD_SSCDPP4	The TSF shall provide CGA[266] with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

7.1.3.7. SFRs for [SSCDPP5]

FDP_UIT.1/DTBS_SSCDPP5	**Data exchange integrity**
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control. fulfilled by FDP_ACC.1/Signature-creation_SSCDPP FTP_ITC.1 Inter-TSF trusted channel or FTP_TRP.1 Trusted path. fulfilled by FTP_ITC.1/DTBS_SSCDPP5
FDP_UIT.1.1/DTBS_SSCDPP5	The TSF shall enforce the Signature Creation SFP[267] to receive[268] user data in a manner protected from modification and insertion[269] errors.
FDP_UIT.1.2/DTBS_SSCDPP5	The TSF shall be able to determine on receipt of user data, whether modification and insertion[270] has occurred.

7.1.4. Class FTP

7.1.4.1. SFRs for [MR.ED-ON-PP]

[265] [assignment: *list of objects or information types*]
[266] [assignment: *list of subjects*]
[267] [assignment: *access control SFP(s) and/or information flow control SFP(s)*]
[268] [selection: *transmit, receive*]
[269] [selection: *modification, deletion, insertion, replay*]
[270] [selection: *modification, deletion, insertion, replay*]

FTP_ITC.1/UPD **Inter-TSF trusted Channel**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/UPD The TSF shall provide a communication channel between itself and ~~*another trusted IT product*~~ ***an update terminal***[271] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/UPD The TSF shall permit ~~*another trusted IT product*~~ ***an update terminal***[272] to initiate communication via the trusted channel.

FTP_ITC.1.3/UPD The TSF shall ~~*initiate*~~ ***enforce*** communication via the trusted channel for *any data exchange between the TOE and the update terminal*.[273]

7.1.4.2. SFRs for [EAC2PP]

The following two SFRs are imported from [EAC2PP].

FTP_ITC.1/PACE_EAC2PP **Inter-TSF trusted channel after PACE**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/PACE_EAC2PP The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **a PACE terminal** that is logically distinct from other communication channels and provides

[271] [selection: *the TSF, another trusted IT product*]
[272] [selection: *the TSF, another trusted IT product*]
[273] [assignment: *list of functions for which a trusted channel is required*]

assured identification of its end points and protection of the channel data from modification or disclosure. **The trusted channel shall be established by performing the PACE protocol according to [TR03110-2]**.

FTP_ITC.1.2/PACE_EAC2PP The TSF shall permit ~~another trusted IT product~~ **a PACE terminal**[274] to initiate communication via the trusted channel.

FTP_ITC.1.3/PACE_EAC2PP The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and **a PACE terminal after PACE**.[275]

Application note 85*:* The above definition refines FTP_ITC.1 from [PACEPP]. The definitions there are unclear as to what the "other trusted IT product" actually is. Since we distinguish here between trusted channels that are established once after PACE, and then then (re)established after CA2, the above refinement is necessary for clarification.

FTP_ITC.1/CA2_EAC2PP Inter-TSF trusted channel after CA2

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/CA2_EAC2PP The TSF shall provide a communication channel between itself and ~~another trusted IT product~~ **an EAC2 terminal** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. **The trusted channel shall be established by performing the CA2 protocol according to [TR03110-2]**.

FTP_ITC.1.2/CA2_EAC2PP The TSF shall permit ~~another trusted IT product~~ **an EAC2 terminal**[276] to initiate communication via the trusted channel.

FTP_ITC.1.3/CA2_EAC2PP The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for any data exchange between the TOE and an EAC2 terminal after Chip Authentication 2.[277]

[274] [selection: *the TSF, another trusted IT product*]
[275] [assignment: *list of functions for which a trusted channel is required*]
[276] [selection: *the TSF, another trusted IT product*]
[277] [assignment: *list of functions for which a trusted channel is required*]

Application note 86: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE_EAC2PP), the TA2 protocol (FIA_UAU.1/EAC2_Terminal_EAC2PP) and the CA2 protocol (FIA_API.1/CA_EAC2PP). If Chip Authentication 2 was successfully performed, secure messaging is immediately restarted using the derived session keys (CA-K_{MAC}, CA-K_{Enc})[278]. This secure messaging enforces the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC_EAC2PP and FCS_COP.1/PACE_MAC_EAC2PP.

7.1.4.3. SFRs for [EAC1PP]

The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

FTP_ITC.1/PACE_EAC1PP **Inter-TSF trusted channel after PACE**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FTP_ITC.1.1/PACE_EAC1PP	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/PACE_EAC1PP	The TSF shall permit another trusted IT product[279] to initiate communication via the trusted channel.
FTP_ITC.1.3/PACE_EAC1PP	The TSF shall ~~initiate~~ **enforce** communication via the trusted channel for <u>any data exchange between the TOE and the Terminal</u>[280].

Application note 87: The trusted IT product is the terminal. In FTP_ITC.1.3/PACE_EAC1PP, the word “initiate” is changed to ‘enforce”, as the TOE is a passive device that can not initiate the communication. All the communications are initiated by the Terminal, and the TOE enforce the trusted channel.

[278] otherwise secure messaging is continued using the established PACE session keys, cf. FTP_ITC.1/PACE_EAC2PP
[279] [selection: *the TSF, another trusted IT product*]
[280] [assignment: *list of functions for which a trusted channel is required*]

Application note 88: The trusted channel is established after successful performing the PACE protocol (FIA_UAU.1/PACE_EAC1PP). If the PACE was successfully performed, secure messaging is immediately started using the derived session keys (PACE-K_{MAC}, PACE-K_{Enc}): this secure messaging enforces preventing tracing while Passive Authentication and the required properties of operational trusted channel; the cryptographic primitives being used for the secure messaging are as required by FCS_COP.1/PACE_ENC_EAC1PP and FCS_COP.1/PACE_MAC_EAC1PP. The establishing phase of the PACE trusted channel does not enable tracing due to the requirements FIA_AFL.1/PACE_EAC1PP.

Application note 89: Please note that the control on the user data stored in the TOE is addressed by FDP_ACF.1/TRM_EAC1PP.

7.1.4.4. SFRs for [SSCDPP4]

The following SFRs is imported due to claiming [SSCDPP4].

FTP_ITC.1/SVD_SSCDPP4	**Inter-TSF trusted channel**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/SVD_SSCDPP4	The TSF shall provide a communication channel between itself and another trusted IT product **CGA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/SVD_SSCDPP4	The TSF shall permit another trusted IT product[281] to initiate communication via the trusted channel.
FTP_ITC.1.3/SVD_SSCDPP4	The TSF **or the CGA** shall initiate communication via the trusted channel for 1) data Authentication with Identity of Guarantor according to FIA_API.1/SSCDPP4 and FDP_DAU.2/SVD_SSCDPP4, 2) *signature verification and VAD verification*[282].

Application note 90: The component FPT_ITC.1/SVD_SSCDPP4 requires the TSF to enforce a trusted channel established by the CGA to export the SVD to the CGA. The ST has performed the missing operations in the element FTP_ITC.1.3/SVD_SSCDPP4.

[281] [selection: the TSF, another trusted IT product]
[282] [assignment: *list of functions for which a trusted channel is required*]

Application note 91: If the ST writer requires the TSF to support (not to enforce) a trusted channel established by the CGA to export the SVD to the CGA than he or she shall use the [SSCDPP] and include a similar component FPT_ITC.1/SVD_SSCDPP4 with assignment "none" in the element FPT_ITC.1.3/SVD_SSCDPP4.

7.1.4.5. SFRs for [SSCDPP5]

The following SFRs are imported due to claiming [SSCDPP5].

FTP_ITC.1/VAD_SSCDPP5	**Inter-TSF trusted channel – TC Human Interface Device**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1/VAD_SSCDPP5	The TSF shall provide a communication channel between itself and another trusted IT product **HID** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/VAD_SSCDPP5	The TSF shall permit the remote trusted IT product[283] to initiate communication via the trusted channel.
FTP_ITC.1.3/VAD_SSCDPP5	The TSF **or the HID** shall initiate communication via the trusted channel for (1) User authentication according to FIA_UAU.1/SSCDPP, (2) *signature verification and SVD export*[284].

Application note 92: The component FTP_ITC.1/VAD_SSCDPP5 requires the TSF to support a trusted channel established by the HID to send the VAD. The ST writer has performed the missing operations in the element FTP_ITC.1.3/VAD_SSCDPP5. Note the VAD needs protection depending on the authentication methods employed: VAD for authentication by knowledge needs protection in confidentiality; VAD for biometric authentication may need protection in integrity only.

FTP_ITC.1/DTBS_SSCDPP5	**Inter-TSF trusted channel – Signature creation Application**
Hierarchical to:	No other components.
Dependencies:	No dependencies.

[283] [selection: the TSF, another trusted IT product]
[284] [assignment: *list of functions for which a trusted channel is required*]

FTP_ITC.1.1/DTBS_SSCDPP5	The TSF shall provide a communication channel between itself and another trusted IT product **SCA** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.
FTP_ITC.1.2/DTBS_SSCDPP5	The TSF shall permit the remote trusted IT product[285] to initiate communication via the trusted channel.
FTP_ITC.1.3/DTBS_SSCDPP5	The TSF **or the SCA** shall initiate communication via the trusted channel for (1) signature creation (2) *signature verification and SVD export*[286].

Application note 93: The component FTP_ITC.1/DTBS_SSCDPP5 requires the TSF to support a trusted channel established by the SCA to send the DTBS. The ST writer has performed the missing operations in the element FTP_ITC.1.3/DTBS_SSCDPP5.

7.1.5. Class FAU

7.1.5.1. SFRs for [MR.ED-ON-PP]

FAU_SAS.1/UPD **Audit Storage of Update History**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FAU_SAS.1.1/UPD	The TSF shall provide ***the TOE update functionality***[287] with the capability to store *update log information and version history, namely the following data objects: OS version coded on the*

[285] [selection: the TSF, another trusted IT product]
[286] [assignment: *list of functions for which a trusted channel is required*]
[287] [assignment: *authorized users*]

ATS, hash of the OS loaded retrieved on the Get Chip Info APDU[288] in the audit records.

Justification: According to [CC], a PP author is allowed to refine an SFR to apply to some, but not all subjects. The refinement of this SFR is such an exception, since the TOE update functionality is technically not an authorized user. Hence, the refinement is justified.

Note FAU_SAS.1 from [MR.ED-PP] applies as well. The SFR here is a new iteration refining the definition of [CC] and is only concerned with the TOE update functionality.

7.1.5.2. SFRs for [EAC2PP]

The following SFR is imported due to claiming [EAC2PP]. It concerns applications with EAC2-protected data.

FAU_SAS.1/EAC2PP **Audit storage**

Hierarchical to:

No other components

Dependencies:

No dependencies

FAU_SAS.1.1/EAC2PP The TSF shall provide the Manufacturer[289] with the capability to store the Initialization and Pre-personalization Data[290] in the audit records.

Application note 94: The Manufacturer role is the default user identity assumed by the TOE in the life cycle phase 'manufacturing'. The IC manufacturer and the travel document manufacturer in the Manufacturer role write the Initialization and/or Pre-personalization Data as TSF-data into the TOE. The audit records are usually write-only-once data of the travel document (see FMT_MTD.1/INI_ENA_EAC2PP, FMT_MTD.1/INI_DIS_EAC2PP). Please note that there could also be such audit records which cannot be read out, but directly used by the TOE.

7.1.5.3. SFRs for [EAC1PP]

The following SFR is imported due to claiming [EAC1PP]. It concerns applications with EAC1-protected data.

FAU_SAS.1/EAC1PP **Audit storage**

(equivalent to FAU_SAS.1/EAC2PP, but listed here for the sake of completeness)

[288] [assignment: *list of audit information*]
[289] [assignment: *authorised users*]
[290] [assignment: *list of audit information*]

7.1.6. Class FMT

7.1.6.1. SFRs for [MR.ED-PP]

FMT_SMR.1 Security roles

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification:

fulfilled by FIA_UID.1/PACE_EAC1PP, FIA_UID.1/PACE_EAC2PP, FIA_UID.1/EAC2_Terminal_EAC2PP, see also the Application Note below.

FMT_SMR.1.1 The TSF shall maintain the roles

1. *Manufacturer,*
2. *Personalization Agent,*
3. *Country Verifying Certification Authority,*
4. *Document Verifier,*
5. *Terminal,*
6. *PACE terminal,*
7. *EAC2 terminal, if the eID, ePassport and/or eSign application are active,*
8. *EAC1 terminal, if the ePassport application is active*
9. *Electronic document holder.*[291]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

The following SFRs concern loading applications onto the IC during manufacturing and relate directly to OT.Cap_Avail_Loader.

FMT_LIM.1/Loader Limited Capabilities

Hierarchical to:

[291] [assignment: *the authorized identified roles*]

No other components

Dependencies:

FMT_LIM.2/Loader Limited availability

fulfilled by FMT_LIM.2/Loader

FMT_LIM.1.1/Loader

The TSF shall be designed and implemented in a manner that limits their capabilities so that in conjunction with "Limited availability (FMT_LIM.2)" the following policy is enforced: *Deploying Loader functionality after delivery*[292] *does not allow stored user data to be disclosed or manipulated by unauthorized users.*[293]

Application note 95*:* FMT_LIM.1/Loader supplements FMT_LIM.2/Loader allowing for non-overlapping loading of user data and protecting the TSF against misuses of the Loader for attacks against the TSF. The TOE Loader may allow for correction of already loaded user data before the assigned action e.g. before blocking the TOE Loader for TOE Delivery to the end-customer or any intermediate step on the life cycle of the Security IC or the smartcard.

FMT_LIM.2/Loader Limited Availability

Hierarchical to:

No other components

Dependencies:

FMT_LIM.1/Loader Limited capabilities

fulfilled by FMT_LIM.1/Loader

FMT_LIM.2.1/Loader

The TSF shall be designed and implemented in a manner that limits their availability so that in conjunction with "Limited capabilities (FMT_LIM.1)" the following policy is enforced: *The TSF prevents deploying the Loader functionality after blocking of the loader*.[294]

Application note 96: The Loader functionality relies on a secure boot loading procedure in a secure environment before TOE delivery to the assigned user and preventing to deploy the

[292] [assignment: *action*]
[293] [assignment: *Limited capability and availability policy*]
[294] [assignment: *Limited capability and availability policy*]

Loader of the Security IC after an assigned action, e.g. after blocking the Loader for TOE delivery to the end-user.

7.1.6.2. SFRs for [MR.ED-ON-PP]

FMT_SMF.1/UPD **Specification of Management Functions including Updates**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FMT_SMF.1.1/UPD The TSF shall be capable of performing the following management functions:

1) *Updating the TOE software with the mechanism specified in [GOA]*[295] [296].

FMT_MTD.1/UPD_SK_PICC **Management of TSF Data – Secret Update Keys**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions:

fulfilled by FMT_SMF.1/UPD

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/UPD

FMT_MTD.1.1/UPD_SK_PICC The TSF shall restrict the ability to *create, load*[297] the *session update keys*[298] to *the update key installation agent*[299].

[295] [assignment: *list of technical specification(s) defining an update mechanism*]
[296] [assignment: *list of management functions to be provided by the TSF*]
[297] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]]

FMT_MTD.1/UPD_KEY_READ **Management of TSF data – Secret Update Keys**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/UPD

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/UPD

FMT_MTD.1.1/UPD_KEY_READ The TSF shall restrict the ability to *read*[300] the

1) *Update keys*[301]
2) *Any data involved in the updating*.[302]

to *none*[303].

FMT_SMR.1/UPD **Security roles**

Hierarchical to:

No other components.

Dependencies:

FIA_UID.1 Timing of identification:

fulfilled by FIA_UID.1/UPD

FMT_SMR.1.1/UPD The TSF shall maintain the roles

---

[298] [assignment: *list of TSF data*]
[299] [assignment: *the authorized identified roles*]
[300] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[301] [assignment: *list of or reference specifying the Secret Cryptographic Update Keys required for the update procedure*]
[302] [assignment: *list of TSF data*]
[303] [assignment: *the authorized identified roles*]

1) *terminal,*
2) *update terminal*
3) *update key installation agent*
4) *Administrator*[304]

FMT_SMR.1.2/UPD The TSF shall be able to associate users with roles.

7.1.6.3. SFRs for [EAC2PP]

The next SFRs are imported from [EAC2PP]. They concern mainly applications with EAC2-protected data.

FMT_MTD.1/CVCA_INI_EAC2PP **Management of TSF data – Initialization of CVCA Certificate and Current Date**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions:

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/CVCA_INI_EAC2PP The TSF shall restrict the ability to write[305] the

1. initial CVCA Public Key,
2. meta-data of the initial CVCA Certificate as required in [TR03110-2], resp. [TR03110-3],
3. initial Current Date
4. *none*[306]

to *the manufacturer*[307].

[304] [assignment: *the authorized identified roles*]
[305] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[306] [assignment: *list of TSF data*]
[307] [assignment: *the authorized identified roles*]

Application note 97: The initial CVCA Public Key may be written by the manufacturer in the manufacturing phase or by the personalization agent in the issuing phase (cf. [TR03110-2]). The initial CVCA Public Keys and their updates later on are used to verify the CVCA Link-Certificates.

FMT_MTD.1/CVCA_UPD_EAC2PP **Management of TSF data – Country Verifying Certification Authority**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/CVCA_UPD_EAC2PP The TSF shall restrict the ability to update[308] the

1. CVCA Public Key (PK_{CVCA}),
2. meta-data of the CVCA Certificate as required by [TR03110-2] , resp. [TR03110-3]
3. *none*[309]

to the Country Verifying Certification Authority.[310]

Application note 98: The CVCA updates its asymmetric key pair and distributes the public key and related meta-data by means of CVCA Link-Certificates. The TOE updates its internal trust-point, if a valid CVCA Link-Certificate (cf. FMT_MTD.3/EAC2PP) is provided by the terminal (cf. [TR03110-3]).

FMT_SMF.1/EAC2PP **Specification of Management Functions**

Hierarchical to:

No other components.

[308] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[309] [assignment: *list of TSF data*]
[310] [assignment: *the authorized identified roles*]

Dependencies:

No dependencies.

FMT_SMF.1.1/EAC2PP The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-Personalization,
3. Personalization,
4. Configuration,
5. **Resume and unblock the PIN (if any)**,
6. **Activate and deactivate the PIN (if any)**[311].

Application note 99: The capability of PIN management gives additional security to the TOE.

Application note 100: The SFR is here refined by including mechanisms for PIN management. A TOE without PIN management functionality can only use a commonly shared secret (such as the MRZ – in the case of an ID document – or the CAN) during execution of PACE to control access to sensitive information. A PIN however must not be shared and thus can be kept secret by the user. Hence, this refinement of FMT_SMF.1/EAC2PP increases protection of user data by allowing PIN access, and thus does not violate strict conformity to [PACEPP].

FMT_SMR.1/PACE_EAC2PP Security roles

This SFR is combined with FMT_SMR.1/PACE_EAC1PP into to by FMT_SMR.1 above.

FMT_SMR.1.1/PACE_EAC2PP

As FMT_SMR.1/PACE_EAC2PP has been combined with FMT_SMR.1/PACE_EAC1PP into FMT_SMR.1, FMT_SMR.1.1/PACE_EAC2PP is included in FMT_SMR.1.1.

FMT_SMR.1.2/PACE_EAC2PP

As FMT_SMR.1/PACE_EAC2PP has been combined with FMT_SMR.1/PACE_EAC1PP into FMT_SMR.1, FMT_SMR.1.2/PACE_EAC2PP is included in FMT_SMR.1.2.

[311] [assignment: *list of management functions to be provided by the TSF*]

FMT_MTD.1/DATE_EAC2PP **Management of TSF data – Current date**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/DATE_EAC2PP The TSF shall restrict the ability to modify[312] the current date[313] to

1. CVCA,
2. Document Verifier
3. EAC2 terminal (Inspection system, authentication terminal, signature terminal) possessing an Accurate Terminal Certificate according to [TR03110-3]
4. *none*[314].

Application note 101: The authorized roles are identified in their certificates (cf. [TR03110-2]) and are authorized by validating the certificate chain up to the CVCA (cf. FMT_MTD.3). The authorized role of a terminal is part of the Certificate Holder Authorization in the card verifiable certificate that is provided by the terminal within Terminal Authentication 2 (cf. [TR03110-3]).

FMT_MTD.1/PA_EAC2PP **Management of TSF data – Personalization Agent**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

[312] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]]
[313] [assignment: *list of TSF data*]
[314] [assignment: *the authorized identified roles*]

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/PA_EAC2PP — The TSF shall restrict the ability to write[315] the **card/chip security object(s) (SO_C) and** the document Security Object (SO_D)[316] to the Personalization Agent[317].

Application note 102: Note that the card/chip security objects are mentioned here as well. These contain information, such as algorithm identifiers, only necessary for EAC2. All requirements formulated in [PACEPP] are thus met, and strict conformance is therefore not violated.

FMT_MTD.1/SK_PICC_EAC2PP — Management of TSF data – Chip Authentication and Restricted Identification Private Key(s)

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions:

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/SK_PICC_EAC2PP — The TSF shall restrict the ability to *create and load*[318] the Chip Authentication private key(s) (SK_{PICC}) ~~***and the Restricted Identification Private Key(s)***[319]~~ to the Personalization Agent[320].

[315] [selection: *change_default, query, modify, delete, clear, [assignment: other operations*]]
[316] [assignment: *list of TSF data*]
[317] [assignment: *the authorized identified roles*]
[318] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[319] [assignment: *list of TSF data*]
[320] [assignment: the authorized identified roles]

Application note 103: The component FMT_MTD.1/SK_PICC_EAC2PP is refined by (i) selecting other operations and (ii) defining a selection for the operations 'create' and 'load'. The verb 'load' means here that the Chip Authentication private key(s) are securely generated outside the TOE and written into the TOE memory. The verb 'create' means here that the Chip Authentication private key(s) are generated by the TOE itself. In the latter case, the ST writer has included an appropriate instantiation of the component FCS_CKM.1/CA_EAC1PP as an SFR for this key generation.

FMT_MTD.1/KEY_READ_EAC2PP Management of TSF data – Private Key Read

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/KEY_READ_EAC2PP The TSF shall restrict the ability to read[321] the

1. PACE passwords,
2. Personalization Agent Keys,
3. the Chip Authentication private key(s) (SK_{PICC})
4. ~~***the Restricted Identification private key(s)***~~
5. *none*[322]

to none[323].

Application note 104: FMT_MTD.1/KEY_READ_EAC2PP extends the SFR from [PACEPP] by additional assignments.

FMT_MTD.1/Initialize_PIN_EAC2PP Management of TSF data – Initialize PIN

Hierarchical to:

[321] [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]]
[322] [assignment: *list of TSF data*]
[323] [assignment: *the authorized identified roles*]

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/Initialize_PIN_EAC2PP	The TSF shall restrict the ability to write[324] the initial PIN and PUK[325] to the personalization agent[326].

FMT_MTD.1/Change_PIN_EAC2PP	**Management of TSF data – Changing PIN**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/Change_PIN_EAC2PP	The TSF shall restrict the ability to change[327] the blocked PIN[328] to *the authorised identified roles that match the list of PIN changing rules conformant to [TR03110-2*]][329]

[324] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[325] [assignment: *list of TSF data*]
[326] [assignment: *the authorized identified roles*]
[327] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[328] [assignment: *list of TSF data*]
[329] [assignment: *the authorized identified roles*]

FMT_MTD.1/Resume_PIN_EAC2PP **Management of TSF data – Resuming PIN**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/Resume_PIN_EAC2PP	The TSF shall restrict the ability to resume[330] the suspended PIN[331] to the electronic document holder[332].

Application note 105: Resuming is a two-step procedure, subsequently using PACE with the CAN and PACE with the PIN. It must be implemented according to [TR03110-2], and is relevant for the status as required by FIA_AFL.1/Suspend_PIN_EAC2PP. The electronic document holder is authenticated as required by FIA_UAU.1/PACE_EAC2PP using the PIN as the shared password.

FMT_MTD.1/Unblock_PIN_EAC2PP **Management of TSF data – Unblocking PIN**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

[330] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[331] [assignment: *list of TSF data*]
[332] [assignment: *the authorized identified roles*]

FMT_MTD.1.1/Unblock_PIN_EAC2PP	The TSF shall restrict the ability to unblock[333] the blocked PIN[334] to 1. the electronic document holder (using the PUK for unblocking), 2. an EAC2 terminal of a type that has the terminal authorization level for PIN management.[335]

Application note 106: The unblocking procedure must be implemented according to [TR03110-2], and is relevant for the status as required by FIA_AFL.1/Block_PIN_EAC2PP. It can be triggered by either (i) the electronic document holder being authenticated as required by FIA_UAU.1/PACE_EAC2PP using the PUK as the shared password or (ii) an EAC2 terminal (FIA_UAU.1/EAC2_Terminal_EAC2PP) that proved a terminal authorization level being sufficient for PIN management (FDP_ACF.1/TRM_EAC2PP).

FMT_MTD.1/Activate_PIN_EAC2PP	**Management of TSF data – Activating/Deactivating PIN**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/Activate_PIN_EAC2PP	The TSF shall restrict the ability to activate and deactivate[336] the PIN[337] to an EAC2 terminal of

[333] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[334] [assignment: *list of TSF data*]
[335] [assignment: *the authorized identified roles*]
[336] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[337] [assignment: *list of TSF data*]

a type that has the terminal authorization level for PIN management[338].

Application note 107: The activation/deactivation procedures must be implemented according to [TR03110-2]. They can be triggered by an EAC2 terminal (FIA_UAU.1/EAC2_Terminal_EAC2PP) that proved a terminal authorization level sufficient for PIN management (FDP_ACF.1/TRM_EAC2PP).

FMT_MTD.3/EAC2PP **Secure TSF data**

Hierarchical to:

No other components.

Dependencies:

FMT_MTD.1 Management of TSF data

fulfilled by FMT_MTD.1/CVCA_INI_EAC2PP, FMT_MTD.1/CVCA_UPD_EAC2PP and FMT_MTD.1/DATE_EAC2PP

FMT_MTD.3.1/EAC2PP The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication protocol 2 and the Access Control SFP[339].

Refinement: To determine if the certificate chain is valid, the TOE shall proceed the certificate validation according to [TR03110-3].

Application note 108: Terminal Authentication is used as required by (i) FIA_UAU.1/EAC2_Terminal_EAC2PP and FIA_UAU.5/PACE_EAC2PP. The terminal authorization level derived from the CVCA Certificate, the DV Certificate and the Terminal Certificate is used as TSF-data for the access control required by FDP_ACF.1/TRM_EAC2PP.

FMT_LIM.1/EAC2PP **Limited capabilities**

Hierarchical to:

No other components

Dependencies:

[338] [assignment: *the authorized identified roles*]
[339] [assignment: *list of TSF data*]

FMT_LIM.2 Limited availability

fulfilled by FMT_LIM.1/EAC2PP

FMT_LIM.1.1/EAC2PP The TSF shall be designed in a manner that limits their capabilities so that in conjunction with 'Limited availability (FMT_LIM.2/EAC2PP)' the following policy is enforced

Deploying Test Features after TOE Delivery do not allow,

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed,
4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed*[340].

Application note 109: The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

FMT_LIM.2/EAC2PP Limited availability

Hierarchical to:

No other components

Dependencies:

FMT_LIM.1 Limited capabilities

fulfilled by FMT_LIM.2/EAC2PP

FMT_LIM.2.1/EAC2PP The TSF shall be designed in a manner that limits their availability so that in conjunction with 'Limited capabilities (FMT_LIM.1/EAC2PP)' the following policy is enforced

Deploying Test Features after TOE Delivery do not allow,

1. User Data to be manipulated and disclosed,
2. TSF data to be manipulated or disclosed,
3. software to be reconstructed,

[340] [assignment: *Limited capability and availability policy*]

4. substantial information about construction of TSF to be gathered which may enable other attacks and
5. *sensitive User Data (EF.DG3 and EF.DG4) to be disclosed*[341].

Application note 110: The functional requirements FMT_LIM.1/EAC2PP and FMT_LIM.2/EAC2PP assume existence of two types of mechanisms (limited capabilities and limited availability) which together shall provide protection in order to enforce the related policy. This also allows that

i. the TSF is provided without restrictions in the product in its user environment, but its capabilities are so limited that the policy is enforced

or conversely

ii. the TSF is designed with high functionality, but is removed or disabled in the product in its user environment.

The combination of both the requirements shall enforce the related policy.

Application note 111: The above SFR concerns the whole TOE, not just applications with EAC2-protected data.

FMT_MTD.1/INI_ENA_EAC2PP **Management of TSF data – Writing Initialisation and Pre-personalisation Data**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions:

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/INI_ENA_EAC2PP The TSF shall restrict the ability to write[342] the Initialisation Data and Pre-personalisation Data[343] to the Manufacturer.[344]

[341] [assignment: *Limited capability and availability policy*]

FMT_MTD.1/INI_DIS_EAC2PP **Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions:

fulfilled by FMT_SMF.1/EAC2PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC2PP

FMT_MTD.1.1/INI_DIS_EAC2PP The TSF shall restrict the ability to read out[345] the Initialisation Data and the Pre-personalisation Data[346] to the Personalisation Agent.[347]

7.1.6.4. SFRs for [EAC1PP]

The following SFRs are imported due to claiming [EAC1PP]. They mainly concern applications with EAC1-protected data.

FMT_SMF.1/EAC1PP **Specification of Management Functions**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

[342] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[343] [assignment: *list of TSF data*]
[344] [assignment: *the authorised identified roles*]
[345] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[346] [assignment: *list of TSF data*]
[347] [assignment: *the authorised identified roles*]

FMT_SMF.1.1/EAC1PP The TSF shall be capable of performing the following management functions:

1. Initialization,
2. Pre-personalisation,
3. Personalisation
4. Configuration.[348]

FMT_SMR.1/PACE_EAC1PP Security roles

This SFR is combined with FMT_SMR.1/PACE_EAC2PP into FMT_SMR.1 above.

FMT_SMR.1.1/PACE_EAC1PP

As FMT_SMR.1/PACE_EAC1PP has been combined with FMT_SMR.1/PACE_EAC2PP into FMT_SMR.1, FMT_SMR.1.1/PACE_EAC1PP is included in FMT_SMR.1.1.

FMT_SMR.1.2/PACE_EAC1PP

As FMT_SMR.1/PACE_EAC1PP has been combined with FMT_SMR.1/PACE_EAC2PP into FMT_SMR.1, FMT_SMR.1.2/PACE_EAC1PP is included in FMT_SMR.1.2.

FMT_LIM.1/EAC1PP Limited capabilities

This SFR is equivalent to FMT_LIM.1/EAC2PP, but listed here for the sake of completeness.

FMT_LIM.2/EAC1PP Limited availability

This SFR is equivalent to FMT_LIM.2/EAC2PP, but listed here for the sake of completeness.

FMT_MTD.1/INI_ENA_EAC1PP Management of TSF data – Writing Initialisation and Pre-personalisation Data

This SFR is equivalent to FDP_MTD.1/INI_ENA_EAC2PP, but listed here for the sake of completeness

[348] [assignment: *list of management functions to be provided by the TSF*]

FMT_MTD.1/INI_DIS_EAC1PP **Management of TSF data – Reading and Using Initialisation and Pre-personalisation Data**

This SFR is equivalent to FMT_MTD.1/INI_DIS_EAC2PP, but listed here for the sake of completeness

Application note 112: The TOE may restrict the ability to write the Initialisation Data and the Pre-personalisation Data by (i) allowing writing these data only once and (ii) blocking the role Manufacturer at the end of the manufacturing phase. The Manufacturer may write the Initialisation Data (as required by FAU_SAS.1) including, but being not limited to a unique identification of the IC being used to trace the IC in the life cycle phases 'manufacturing' and 'issuing', but being not needed and may be misused in the 'operational use'. Therefore, read and use access to the Initialisation Data shall be blocked in the 'operational use' by the Personalisation Agent, when he switches the TOE from the life cycle phase 'issuing' to the life cycle phase 'operational use'.

FMT_MTD.1/CVCA_INI_EAC1PP **Management of TSF data – Initialization of CVCA Certificate and Current Date**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC1PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC1PP

FMT_MTD.1.1/CVCA_INI_EAC1PP The TSF shall restrict the ability to write[349] the

1. initial Country Verifying Certification Authority Public Key,
2. initial Country Verifying Certification Authority Certificate,
3. initial Current Date
4. *none*[350],

[349] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[350] [assignment: *list of TSF data*]

to *the Personalisation Agent*[351].

Application note 113*:* The ST writer has performed the missing operation in the component FMT_MTD.1.1/CVCA_INI_EAC1PP. The initial Country Verifying Certification Authority Public Keys (and their updates later on) are used to verify the Country Verifying Certification Authority Link-Certificates. The initial Country Verifying Certification Authority Certificate and the initial Current Date is needed for verification of the certificates and the calculation of the Terminal Authorization.

FMT_MTD.1/CVCA_UPD_EAC1PP **Management of TSF data – Country Verifying Certification Authority**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC1PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC1PP

FMT_MTD.1.1/CVCA_UPD_EAC1PP The TSF shall restrict the ability to update[352] the

1. Country Verifying Certification Authority Public Key,
2. Country Verifying Certification Authority Certificate[353]

to Country Verifying Certification Authority[354].

Application note 114: The Country Verifying Certification Authority updates its asymmetric key pair and distributes the public key be means of the Country Verifying CA Link-Certificates (cf.

[351] [assignment: *the authorised identified roles*]
[352] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[353] [assignment: *list of TSF data*]
[354] [assignment: *the authorised identified roles*]

[TR03110]). The TOE updates its internal trust-point if a valid Country Verifying CA Link-Certificates (cf. FMT_MTD.3/EAC1PP) is provided by the terminal (cf. [TR03110]).

FMT_MTD.1/DATE_EAC1PP **Management of TSF data – Current**

This SFR is equivalent to FMT_MTD.1/DATE_EAC2PP. Note that FMT_MTD.1/DATE_EAC2PP generalizes the notion of Domestic Extended Inspection System to EAC1 terminals with appropriate authorization level. This does not violate strict conformance to [EAC1PP].

FMT_MTD.1/CAPK_EAC1PP **Management of TSF data – Chip Authentication Private Key**

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC1PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC1PP

FMT_MTD.1.1/CAPK_EAC1PP The TSF shall restrict the ability to *create and load*[355] the Chip Authentication Private Key[356] to *the Personalisation Agent*[357].

Application note 115: The component FMT_MTD.1/CAPK_EAC1PP is refined by (i) selecting other operations and (ii) defining a selection for the operations “create” and “load” to be performed by the ST writer. The verb “load” means here that the Chip Authentication Private Key is generated securely outside the TOE and written into the TOE memory. The verb “create” means here that the Chip Authentication Private Key is generated by the TOE itself. In the latter case the ST writer shall include an appropriate instantiation of the component FCS_CKM.1/CA_EAC1PP as SFR for this key generation. The ST writer has performed the

[355] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[356] [assignment: *list of TSF data*]
[357] [assignment: *the authorised identified roles*]

assignment for the authorized identified roles in the SFR component FMT_MTD.1/CAPK_EAC1PP.

FMT_MTD.1/PA_EAC1PP Management of TSF data – Personalisation Agent

This SFR is equivalent to FMT_MTD.1/PA_EAC2PP, but listed here for the sake of completeness

Application note 116: By writing SOD into the TOE, the Personalisation Agent confirms (on behalf of DS) the correctness and genuineness of all the personalisation data related. This consists of user- and TSF- data.

FMT_MTD.1/KEY_READ_EAC1PP Management of TSF data – Key Read

Hierarchical to:

No other components.

Dependencies:

FMT_SMF.1 Specification of management functions

fulfilled by FMT_SMF.1/EAC1PP

FMT_SMR.1 Security roles:

fulfilled by FMT_SMR.1/PACE_EAC1PP

FMT_MTD.1.1/KEY_READ_EAC1PP The TSF shall restrict the ability to read[358] the

1. PACE passwords,
2. Chip Authentication Private Key,
3. Personalisation Agent Keys[359]

to none[360].

Application note 117: The SFR FMT_MTD.1/KEY_READ_EAC1PP in the current ST covers the definition in PACE PP [PACEPP] and extends it by additional TSF data. This extension does not conflict with the strict conformance to PACE PP.

[358] [selection: *change_default, query, modify, delete, clear,* [assignment: *other operations*]]
[359] [assignment: *list of TSF data*]
[360] [assignment: *the authorised identified roles*]

FMT_MTD.3/EAC1PP Secure TSF data

Hierarchical to:

No other components.

Dependencies:

FMT_MTD.1 Management of TSF data

fulfilled by FMT_MTD.1/CVCA_INI_EAC1PP, FMT_MTD.1/CVCA_UPD_EAC1PP and FMT_MTD.1/DATE_EAC1PP

FMT_MTD.3.1/EAC1PP The TSF shall ensure that only secure values **of the certificate chain** are accepted for TSF data of the Terminal Authentication Protocol v.1 and the Access Control[361].

Refinement: The certificate chain is valid if and only if

1. **the digital signature of the Inspection System Certificate can be verified as correct with the public key of the Document Verifier Certificate and the expiration date of the Inspection System Certificate is not before the Current Date of the TOE,**
2. **the digital signature of the Document Verifier Certificate can be verified as correct with the public key in the Certificate of the Country Verifying Certification Authority and the expiration date of the Document Verifier Certificate is not before the Current Date of the TOE,**
3. **the digital signature of the Certificate of the Country Verifying Certification Authority can be verified as correct with the public key of the Country Verifying Certification Authority known to the TOE and the expiration date of the Certificate of the Country Verifying Certification Authority is not before the Current Date of the TOE.**

The Inspection System Public Key contained in the Inspection System Certificate in a valid certificate chain is a secure value for the authentication reference data of the Extended Inspection System.

The intersection of the Certificate Holder Authorizations contained in the certificates of a valid certificate chain is a secure value for Terminal Authorization of a successful authenticated Extended Inspection System.

Application note 118: The Terminal Authentication Version 1 is used for Extended Inspection System as required by FIA_UAU.4/PACE_EAC1PP and FIA_UAU.5/PACE_EAC1PP. The Terminal Authorization is used as TSF data for access control required by FDP_ACF.1/TRM.

[361] [assignment: *list of TSF data*]

7.1.6.5. SFRs for [SSCDPP]

The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the security management of an *eSign* application.

FMT_SMR.1/SSCDPP	**Security roles**
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification fulfilled by FIA_UID.1/SSCDPP
FMT_SMR.1.1/SSCDPP	The TSF shall maintain the roles R.Admin and R.Sigy[362].
FMT_SMR.1.2/SSCDPP	The TSF shall be able to associate users with roles.

FMT_SMF.1/SSCDPP	**Security management functions**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1/SSCDPP	The TSF shall be capable of performing the following management functions: 1. Creation and modification of RAD, 2. Enabling the signature creation function, 3. Modification of the security attribute SCD/SVD management, SCD operational, 4. Change the default value of the security attribute SCD Identifier, 5. *none*[363].

FMT_MOF.1/SSCDPP	**Management of security functions behaviour**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP FMT_SMF.1 Specification of Management Functions. fulfilled by FMT_SMF.1/SSCDPP

[362] [assignment: *the authorised identified roles*]
[363] [assignment: *list of other security management functions to be provided by the TSF*]

FMT_MOF.1.1/SSCDPP	The TSF shall restrict the ability to enable[364] the functions signature creation function[365] to R.Sigy[366].

FMT_MSA.1/Admin_SSCDPP	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/SCD/SVD_Generation_SSCDPP FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP FMT_SMF.1 Specification of Management Functions fulfilled by FMT_SMF.1/SSCDPP
FMT_MSA.1.1/Admin_SSCDPP	The TSF shall enforce the SCD/SVD Generation SFP[367] to restrict the ability to modify[368] the security attributes SCD/SVD management[369] to R.Admin[370].

FMT_MSA.1/Signatory_SSCDPP	**Management of security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/Signature-Creation_SSCDPP FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP FMT_SMF.1 Specification of Management Functions

[364] [selection: *determine the behaviour of, disable, enable, modify the behaviour of*]
[365] [assignment: *list of functions*]
[366] [assignment: *the authorised identified roles*]
[367] [assignment: *access control SFP(s), information flow control SFP(s)*]
[368] [selection: *change_default, query, modify, delete, [*assignment:*other operations*]]
[369] [assignment: *list of security attributes*]
[370] [assignment: *the authorised identified roles*]

	fulfilled by FMT_SMF.1/SSCDPP
FMT_MSA.1.1/Signatory_SSCDPP	The TSF shall enforce the Signature Creation SFP[371] to restrict the ability to modify[372] the security attributes SCD operational[373] to R.Sigy[374].

FMT_MSA.2/SSCDPP	**Secure security attributes**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/SCD/SVD_Generation_SSCDPP and FDP_ACC.1/Signature-Creation_SSCDPP FMT_MSA.1 Management of security attributes fulfilled by FMT_MSA.1/Admin_SSCDPP and FMT_MSA.1/Signatory_SSCDPP FMT_SMR.1 Security roles fulfilled by FMT_SMR.1/SSCDPP
FMT_MSA.2.1/SSCDPP	The TSF shall ensure that only secure values are accepted for SCD/SVD Management and SCD operational[375].

FMT_MSA.3/SSCDPP	**Static attribute initialisation**
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes fulfilled by FMT_MSA.1/Admin_SSCDPP and FMT_MSA.1/Signatory_SSCDPP FMT_SMR.1 Security roles

[371] [assignment: *access control SFP(s), information flow control SFP(s)*]
[372] [selection: *change_default, query, modify, delete, [assignment: other operations*]]
[373] [assignment: *list of security attributes*]
[374] [assignment: *the authorised identified roles*]
[375] [selection: *list of security attributes*]

	fulfilled by FMT_SMR.1/SSCDPP
FMT_MSA.3.1/SSCDPP	The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP[376] to provide restrictive[377] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2/SSCDPP	The TSF shall allow the R.Admin[378] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4/SSCDPP	**Security attribute value inheritance**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] fulfilled by FDP_ACC.1/SCD/SVD_Generation_SSCDPP and FDP_ACC.1/Signature-Creation_SSCDPP
FMT_MSA.4.1/SSCDPP	The TSF shall use the following rules to set the value of security attributes: (1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation. (2) If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation[379].

FMT_MTD.1/Admin_SSCDPP	**Management of TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles

[376] [assignment: *access control SFP, information flow control SFP*]
[377] [selection, choose one of: *restrictive, permissive, [assignment: other property*]]
[378] [assignment: *the authorised identified roles*]
[379] [assignment: *rules for setting the values of security attributes*]

	fulfilled by FMT_SMR.1/SSCDPP
	FMT_SMF.1 Specification of Management Functions
	fulfilled by FMT_SMF.1/SSCDPP
FMT_MTD.1.1/Admin_SSCDPP	The TSF shall restrict the ability to create[380] the RAD[381] to R.Admin[382].

FMT_MTD.1/Signatory_SSCDPP	**Management of TSF data**
Hierarchical to:	No other components.
Dependencies:	FMT_SMR.1 Security roles
	fulfilled by FMT_SMR.1/SSCDPP
	FMT_SMF.1 Specification of Management Functions
	fulfilled by FMT_SMF.1/SSCDPP
FMT_MTD.1.1/Signatory_SSCDPP	The TSF shall restrict the ability to modify *and unblock*[383] the RAD[384] to R.Sigy[385].

7.1.7. Class FPT

7.1.7.1. SFRs for [MR.ED-ON-PP]

FPT_EMS.1/UPD **TOE Emanation**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

[380] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[381] [assignment: *list of TSF data*]
[382] [assignment: *the authorised identified roles*]
[383] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[384] [assignment: *list of TSF data*]
[385] [assignment: *the authorised identified roles*]

FPT_EMS.1.1/UPD The TOE shall not emit *electromagnetic and current emissions*[386] in excess of *intelligible threshold*[387] enabling access to *the update keys*[388] and *any user data*[389].

FPT_EMS.1.2/UPD The TSF shall ensure *any users*[390] are unable to use the following interface *electronic document 's contactless/contact-based interface and circuit contacts*[391] to gain access to *the update keys* [392] and *any user data*[393].

Application note 119: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in power consumption, timing of signals, and electromagnetic radiation due to internal operations or data transmissions.

Note that while the security functionality described in FPT_EMS.1/UPD should be taken into account during development of the TOE, associated tests must be carried out as part of the evaluation, and not/not only during product development.

FPT_FLS.1/UPD Failure with Preservation of Secure State (Failed Update)

Hierarchical to:

No other components.

Dependencies:

No dependencies.

[386] [assignment: *types of emissions*]
[387] [assignment: *specified limits*]
[388] [assignment: *list of types of TSF data*]
[389] [assignment: *list of types of user data*]
[390] [assignment: *type of users*]
[391] [assignment: *type of connection*]
[392] [assignment: *list of types of TSF data*]
[393] [assignment: *list of types of user data*]

FPT_FLS.1.1/UPD The TSF shall preserve a secure state when the following types of failures occur:

1) *Failure during a transmission of the update package data file*
2) *Failure detected by TSF according to FPT_TST.1/UPD*
3) *Failure detected after a failed update*[394]
4) *Wrong digital signature*[395].

Application note 120: The secure state after a failed update should be achieved by reverting to the previous TOE software version. Nevertheless this capability will have limits, since the atomicity of the software update mechanism can technically only be achieved up to a certain extent.

FPT_TST.1/UPD TSF Testing (after Installation of an Update)

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_TST.1.1/UPD The TSF shall run a suite of self tests *during initial start-up*[396] to demonstrate the correct operation of *the TSF*[397].

FPT_TST.1.2/UPD The TSF shall provide authorized users with the capability to verify the integrity *of the TSF data*[398].

FPT_TST.1.3/UPD The TSF shall provide authorized users with the capability to verify the integrity of *stored TSF executable code*[399].

[394] [assignment: *list of types of failures in the TSF*]
[395] [assignment: *list of types of failures in the TSF*]
[396] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions*[assignment: *conditions under which self test should occur*]]
[397] [selection: [assignment*: parts of TSF], the TSF*]
[398] [selection: [assignment: *parts of TSF data], TSF data*]
[399] [selection: [assignment*: parts of TSF], TSF]*

7.1.7.2. SFRs for [EAC2PP]

The following security functional requirements are imported from [EAC2PP], and address the protection against forced illicit information leakage, including physical manipulation.

FPT_EMS.1/EAC2PP **TOE Emanation**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_EMS.1.1/EAC2PP The TOE shall not emit electromagnetic and current emissions[400] in excess of intelligible threshold[401] enabling access to

1. **the** session keys (PACE-K_{MAC}, PACE-K_{Enc}), **(CA-K_{MAC}, CA-K_{Enc}),**
2. the ephemeral private key ephem-SK_{PICC}-PACE[402],
3. the Chip Authentication private keys (SK_{PICC})**,**
4. the PIN, PUK,
5. *none*[403]**,**

and

~~6. the Restricted Identification private key(s) SK_{ID}~~[404]

7. *EF.DG1 to EF.DG22, EF.SOD, EF.COM*[405].

Application note 121: Restricted Identification is not supported by the TOE.

FPT_EMS.1.2/EAC2PP The TSF shall ensure any users[406] are unable to use the following interface electronic document 's contactless/***contact-based interface*** and circuit contacts[407] to gain access to

1. **the** session keys (PACE-K_{MAC}, PACE-K_{Enc}), (**CA-K_{MAC}, CA-K_{Enc}**)
2. the ephemeral private key ephem-SK_{PICC}-PACE1,

[400] [assignment: *types of emissions*]
[401] [assignment: *specified limits*]
[402] [assignment: *list of types of TSF data*]
[403] [assignment: *list of types of TSF data*]
[404] [assignment: *list of types of user data*]
[405] [assignment: *list of types of user data*]
[406] [assignment: *type of users*]
[407] [assignment: *type of connection*]

3. the Chip Authentication private key(s) (SK_{PICC}),
4. the PIN, PUK,
5. *none*[408]

and

6. ~~*the Restricted Identification private key(s) SK_{ID}*~~
7. *EF.DG1 to EF.DG22, EF.SOD, EF.COM.*[409]

Application note 122: Restricted Identification is not supported by the TOE.

Application note 123: The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE, originate from internal operation of the TOE, or be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. Examples of measurable phenomena include, but are not limited to variations in power consumption, timing of signals, and electromagnetic radiation due to internal operations or data transmissions. Note that while the security functionality described in FPT_EMS.1/EAC2PP should be taken into account during development of the TOE, associated tests must be carried out as part of the evaluation, and not/not only during product development. Note that in the above SFR, all items in FPT_EMS.1.2/EAC2PP from 3. upwards are additional assignments. The first item is slightly refined to include CA-key(s).

Application note 124: Note that related to the PIN in the above SFR refers here to both the PIN for an eID application, and also the PIN for an eSign application, if they exist on card.

A refinement is used here to ensure that emissions via contact-based interfaces must not be observable as well. This extends the scope of emission analysis by creating a stricter requirement. Hence, the refinement is justified.

FPT_FLS.1/EAC2PP **Failure with preservation of secure state**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_FLS.1.1/EAC2PP The TSF shall preserve a secure state when the following types of failures occur:

[408] [assignment: *list of types of TSF data*]
[409] [assignment: *list of types of user data*]

1. Exposure to operating conditions causing a TOE malfunction,
2. Failure detected by TSF according to FPT_TST.1/EAC2PP.
3. *none*.[410]

FPT_TST.1/EAC2PP **TSF testing**

Hierarchical to:

No other components.

Dependencies:

No dependencies.

FPT_TST.1.1/EAC2PP	The TSF shall run a suite of self tests *during initial start-up and before any use of TSF data*[411] to demonstrate the correct operation of the TSF[412].
FPT_TST.1.2/EAC2PP	The TSF shall provide authorized users with the capability to verify the integrity of the TSF data[413].
FPT_TST.1.3/EAC2PP	The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code[414].

Application note 125: If the travel document's chip uses state of the art smart card technology, it will run some self tests at the request of an authorized user and some self tests automatically. E.g. a self test for the verification of the integrity of stored TSF executable code required by FPT_TST.1.3/EAC2PP may be executed during initial start-up by the 'authorized user' Manufacturer in the life cycle phase 'Manufacturing'. Other self tests may automatically run to detect failures and to preserve the secure state according to FPT_FLS.1/EAC2PP in the phase 'operational use', e.g. to check a calculation with a private key by the reverse calculation with the corresponding public key as a countermeasure against Differential Failure Analysis.

FPT_PHP.3/EAC2PP **Resistance to physical attack**

Hierarchical to:

[410] [assignment: *list of types of failures in the TSF*]
[411] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [*assignment: conditions under which self test should occur*]]
[412] [selection: *[assignment: parts of TSF], the TSF]*
[413] [selection: *[assignment: parts of TSF], TSF data*]
[414] [selection: *[assignment: parts of TSF], TSF*]

No other components.

Dependencies:

No dependencies.

FPT_PHP.3.1/EAC2PP The TSF shall resist physical manipulation and physical probing[415] to the TSF[416] by responding automatically such that the SFRs are always enforced.

Application note 126: The TOE will implement appropriate measures to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TOE can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that the TSP could not be violated at any time. Hence, 'automatic response' means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.

7.1.7.3. SFRs for [EAC1PP]

The following SFRs are imported due to claiming [EAC1PP]. They mostly concern the protection of security functionality related to EAC1-protected data.

FPT_TST.1/EAC1PP TSF testing

This SFR is equivalent to FPT_TST.1/EAC2PP, but listed here for the sake of completeness.

FPT_FLS.1/EAC1PP Failure with preservation of secure state

This SFR is equivalent to FPT_FLS.1/EAC2PP, but listed here for the sake of completeness.

FPT_PHP.3/EAC1PP Resistance to physical attack

This SFR is equivalent to FPT_PHP.3/EAC2PP, but listed here for the sake of completeness.

FPT_EMS.1/EAC1PP Emanation

Hierarchical to:

[415] [assignment: *physical tampering scenarios*]
[416] [assignment: *list of TSF devices/elements*]

No other components

Dependencies:

No dependencies.

FPT_EMS.1.1/EAC1PP

The TOE shall not emit *electromagnetic and current emissions*[417] in excess of *intelligible threshold*[418] enabling access to

1. Chip Authentication ***(Version 1)*** Session Keys,
2. PACE session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem SK_{PICC}-PACE,
4. *none,*
5. Personalization Agent Key(s),
6. Chip Authentication ***(Version 1)*** Private Key[419] and
7. *EF.DG1 to EF.DG16, EF.SOD and EF.COM*[420]

FPT_EMS.1.2/EAC1PP

The TSF shall ensure any users[421] are unable to use the following interface smart card circuit contacts[422] to gain access to

1. Chip Authentication (***Version 1***) Session Keys
2. PACE Session Keys (PACE-K_{MAC}, PACE-K_{Enc}),
3. the ephemeral private key ephem SK_{PICC}-PACE,
4. *none*[423]
5. Personalization Agent Key(s) and,
6. Chip Authentication (***Version 1***) Private Key[424]
7. *EF.DG1 to EF.DG16, EF.SOD and EF.COM*[425]

Application note 127: The SFR FPT_EMS.1.1/EAC1PP covers the definition in [PACEPP] and extends it by EAC aspects 1., 5. and 6. The SFR FPT_EMS.1.2/EAC1PP covers the definition in [PACEPP] and extends it by EAC aspects 4) and 5). These extensions do not conflict with the strict conformance to [PACEPP].

[417] [assignment: *types of emissions*]
[418] [assignment: *specified limits*]
[419] [assignment: *list of types of TSF data*]
[420] [assignment: *list of types of user data*]
[421] [assignment: *type of users*]
[422] [assignment: *type of connection*]
[423] [assignment: *list of types of TSF data*],
[424] [assignment: *list of types of TSF data*]
[425] [assignment: *list of types of user data*]

Application note 128: The ST writer has performed the operations in FPT_EMS.1.1/EAC1PP and FPT_EMS.1.2/EAC1PP. The TOE shall prevent attacks against the listed secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may be originated from internal operation of the TOE or may be caused by an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the smart card. The travel document's chip can provide a smart card contactless interface and contact based interface according to [ISO7816-2] as well (in case the package only provides a contactless interface the attacker might gain access to the contacts anyway). Examples of measurable phenomena include, but are not limited to variations in the power consumption, the timing of signals and the electromagnetic radiation due to internal operations or data transmissions.

The following security functional requirements address the protection against forced illicit information leakage including physical manipulation.

7.1.7.4. SFRs for [SSCDPP]

The following SFRs are imported due to claiming [SSCDPP]. They mostly concern the protection of security functionality related to eSign application.

FPT_EMS.1/SSCDPP	**TOE Emanation**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMS.1.1/SSCDPP	The TOE shall not emit *electromagnetic and current emissions*[426] in excess of *useless information*[427] enabling access to RAD[428] and SCD[429].
FPT_EMS.1.2/SSCDPP	The TSF shall ensure *attackers*[430] are unable to use the following interface *the contactless interface and circuit contacts*[431] to gain access to RAD[432] and SCD[433].

Application note 129: The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may origin from internal operation of the TOE or may origin by an attacker that varies the physical environment under which the TOE

[426] [assignment: *types of emissions*]
[427] [assignment: *specified limits*]
[428] [assignment: *list of types of TSF data*]
[429] [assignment: *list of additional types of user data*]
[430] [assignment: *type of users*]
[431] [assignment: *type of connection*]
[432] [assignment: *list of types of (further) TSF data*]
[433] [assignment: *list of types of user data*]

operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission.

Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, etc.

FPT_FLS.1/SSCDPP (subsumed by FPT_FLS.1/EAC2PP)	**Failure with preservation of secure state**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1/SSCDPP	The TSF shall preserve a secure state when the following types of failures occur: (1) self-test according to FPT_TST.1/SSCDPP fails, (2) *any communication protocol attack or sensor detection of not detected parameters*[434].

Application note 130: The ST writer has performed the missing assignment in the element FPT_FLS.1.1/SSCDPP. The assignment (1) addresses failures detected by a failed self-test and requiring appropriate action to prevent security violation. When the TOE is in a secure state the TSF shall not perform any cryptographic operations and all data output interfaces shall be inhibited by the TSF.

FPT_PHP.1/SSCDPP	**Passive detection of physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.1.1/SSCDPP	The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.
FPT_PHP.1.2/SSCDPP	The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

[434] [assignment: *list of types of failures in the TSF*]

FPT_PHP.3/SSCDPP (subsumed by FPT_PHP.3/EAC2PP)	**Resistance to physical attack**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1/SSCDPP	The TSF shall resist *physical manipulation and physical probing*[435] to the *TSF*[436] by responding automatically such that the SFRs are always enforced.

Application note 131: The TOE will implement appropriate measures to continuously counter physical tampering which may compromise the SCD. The "automatic response" in the element FPT_PHP.3.1/SSCDPP means (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time. Due to the nature of these attacks the TOE can by no means detect attacks on all of its elements (e.g. the TOE is destroyed). But physical tampering must not reveal information of the SCD. E.g. the TOE may be physically tampered in power-off state of the TOE (e.g. a smart card), which does not allow TSF for overwriting the SCD but leads to physical destruction of the memory and all information therein about the SCD. In case of physical tampering the TFS may not provide the intended functions for SCD/SVD pair generation or signature creation but ensures the confidentiality of the SCD by blocking these functions. The SFR FPT_PHP.1/SSCDPP requires the TSF to react on physical tampering in a way that the signatory is able to determine whether the TOE was physical tampered or not. E.g. the TSF may provide an appropriate message during start-up or the guidance documentation may describe a failure of TOE start-up as indication of physical tampering.

FPT_TST.1/SSCDPP (subsumed by FPT_TST.1/EAC2PP)	**TSF testing**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1/SSCDPP	The TSF shall run a suite of self tests *during initial start-up before any use of TSF data*[437] to demonstrate the correct operation of the TSF[438].

[435] [assignment: *physical tampering scenarios*]
[436] [assignment: *list of TSF devices/elements*]
[437] [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions* [assignment: *conditions under which self-test should occur*]]
[438] [selection: [assignment: *parts of TSF], the TSF*]

FPT_TST.1.2/SSCDPP The TSF shall provide authorised users with the capability to verify the integrity of TSF data[439].

FPT_TST.1.3/SSCDPP The TSF shall provide authorised users with the capability to verify the integrity of TSF[440].

7.2. Security Assurance Requirements for the TOE

The assurance requirements for the evaluation of the TOE, its development and operating environment are to choose as the predefined assurance package EAL4 augmented by the following components:

- ALC_DVS.2 (Sufficiency of security measures),
- ATE_DPT.2 (Testing: security enforcing modules) and
- AVA_VAN.5 (Advanced methodical vulnerability analysis).

Los requisitos de garantía de seguridad se justifican mediante la presentación a la evaluación de los distintos documentos que acreditan el cumplimiento de los correspondientes requisitos.

Componente	Documentos
ADV_ARC.1 Security architecture description	Descripción de la arquitectura de seguridad
ADV_FSP.4 Complete functional specification	Especificación funcional - Manual de comandos
ADV_IMP.1 Implementation representation of the TSF	Código fuente y mapas de ficheros
ADV_TDS.3 Basic modular design	Diseño
AGD_OPE.1 Operational user guidance	Guía operativa para administrador y para usuario final
AGD_PRE.1 Preparative procedures	Guía preparativa
ALC_CMC.4 Production support, acceptance procedures and automation	Plan de gestión de la configuración
ALC_CMS.4 Problem tracking CM coverage	Listado de configuración
ALC_DEL.1 Delivery procedures	Procedimientos de entrega
ALC_DVS.2 Sufficiency of security measures	Medidas de seguridad para de desarrollo
ALC_LCD.1 Developer defined life-cycle model	Ciclo de vida de la tarjeta

[439] [selection: [assignment: *parts of TSF data], TSF data*]
[440] [selection: [assignment: *parts of TSF], TSF*]

ALC_TAT.1 Well-defined development tools	Herramientas y técnicas para el desarrollo del Sistema Operativo
ASE_CCL.1 Conformance claims	Declaración de seguridad
ASE_ECD.1 Extended components definition	
ASE_INT.1 ST introduction	
ASE_OBJ.2 Security objectives	
ASE_REQ.2 Derived security requirements	
ASE_SPD.1 Security problem definition	
ASE_TSS.1 TOE summary specification	
ATE_COV.2 Analysis of coverage	Análisis de la cobertura de las pruebas para la especificación funcional
ATE_DPT.2 Testing: security enforcing modules	Definición de las pruebas de los subsistemas
ATE_FUN.1 Functional testing	Plan de pruebas
ATE_IND.2 Independent testing – sample	Documentación de pruebas
AVA_VAN.5 Advanced methodical vulnerability analysis	Documentación de análisis de vulnerabilidades

Tabla 6.- Documentación y requisitos de garantía de seguridad.

7.3. Security Requirements Rationale

7.3.1. Security Functional Requirements Rationale

The following table provides an overview for the coverage of the security functional requirements, and also gives evidence for sufficiency and necessity of the chosen SFRs.

	OT.Non_Interfere	OT.Cap_Avail_Loader	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FAU_SAS.1/UPD			X			X																															
FAU_SAS.1/EAC2PP										X							X																				
FAU_SAS.1/EAC1PP													X				X																				
FCS_COP.1/UPD_ITC			X	X																																	
FCS_CKM.1/UPD_ITC			X	X																																	
FCS_COP.1/UPD_DEC			X	X																																	
FCS_CKM.1/UPD_DEC			X	X																																	
FCS_COP.1/UPD_SIG			X	X																																	
FCS_COP.1/UPD_INT			X	X																																	
FCS_CKM.1/UPD_INT			X	X																																	
FCS_CKM.4/UPD			X	X																																	
FCS_CKM.4/UPD_OS			X	X																																	
FCS_CKM.1/DH_PACE_EAC2PP											X	X		X	X	X																					
FCS_COP.1/SHA_EAC2PP											X	X		X	X	X																					
FCS_COP.1/SIG_VER_EAC2PP												X		X	X	X																					
FCS_COP.1/PACE_ENC_EAC2PP												X			X																						
FCS_COP.1/PACE_MAC_EAC2PP											X			X		X																					
FCS_CKM.4/EAC2PP												X		X	X	X																					
FCS_RND.1/EAC2PP											X	X		X	X	X																					
FCS_CKM.1/DH_PACE_EAC1PP														X	X	X																					
FCS_CKM.4/EAC1PP									X				X	X	X	X																					
FCS_COP.1/PACE_ENC_EAC1PP															X																						
FCS_COP.1/PACE_MAC_EAC1PP														X		X																					
FCS_RND.1/EAC1PP									X				X	X	X	X																					
FCS_CKM.1/CA_EAC1PP								X	X				X	X	X	X																					
FCS_COP.1/CA_ENC_EAC1PP								X	X				X		X	X																					
FCS_COP.1/SIG_VER_EAC1PP									X				X																								
FCS_COP.1/CA_MAC_EAC1PP								X	X				X			X																					
FCS_CKM.1/RSA_SSCDPP																									X	X	X	X									
FCS_CKM.1/AES_PRO																									X	X	X	X									
FCS_CKM.1/EC_SSCDPP																									X	X	X	X									
FCS_CKM.4/RSA_SSCDPP																									X	X											
FCS_CKM.4/AES_PRO																									X	X											
FCS_CKM.4/EC_SSCDPP																									X	X											
FCS_COP.1/RSA_SSCDPP																									X					X							
FCS_COP.1/AES_PRO																									X					X							
FCS_COP.1/SHA_SSCDPP																									X					X							
FCS_COP.1/EC_SSCDPP																									X					X							
FDP_ACF.1/TRM	X								X	X		X	X		X	X																					
FDP_ACC.1/UPD			X		X																																
FDP_ACF.1/UPD			X		X																																
FDP_IFC.1/UPD			X		X																																
FDP_IFF.1/UPD			X		X																																
FDP_RIP.1/UPD			X																																		
FDP_ACC.1/TRM_EAC2PP										X		X			X	X																					
FDP_ACF.1/TRM_EAC2PP										X		X			X	X																					
FDP_RIP.1/EAC2PP										X	X	X		X	X	X																					
FDP_UCT.1/TRM_EAC2PP												X			X	X																					
FDP_UIT.1/TRM_EAC2PP												X			X	X																					
FDP_ACC.1/TRM_EAC1PP										X			X		X	X																					
FDP_ACF.1/TRM_EAC1PP										X			X		X	X																					
FDP_RIP.1/EAC1PP														X	X	X																					
FDP_UCT.1/TRM_EAC1PP										X					X	X																					
FDP_UIT.1/TRM_EAC1PP															X	X																					
FDP_ACC.1/SCD/SVD_Generation_SSCDPP																									X				X								
FDP_ACF.1/SCD/SVD_Generation_SSCDPP																									X				X								
FDP_ACC.1/SVD_Transfer_SSCDPP																									X												
FDP_ACF.1/SVD_Transfer_SSCDPP																									X												
FDP_ACC.1/Signature_Creation_SSCDPP																									X						X						
FDP_ACF.1/Signature_Creation_SSCDPP																									X						X						
FDP_RIP.1/SSCDPP																										X					X						
FDP_SDI.2/Persistent_SSCDPP																										X	X			X							
FDP_SDI.2/DTBS_SSCDPP																								X							X						
FDP_DAU.2/SVD_SSCDPP4																																					X
FDP_UIT.1/DTBS_SSCDPP5																																			X		
FIA_AFL.1/UPD			X		X																																
FIA_UID.1/UPD			X		X																																

	OT.Non_Interfere	OT.Cap_Avail_Loader	OT.Update_Mechanism	OT.Enc_Sign_Update	OT.Update_Terminal_Auth	OT.Attack_Detection	OT.Key_Secrecy	OT.Chip_Auth_Proof	OT.Sens_Data_Conf	OT.AC_Pers_EAC2	OT.CA2	OT.Sens_Data_EAC2	OT.AC_Pers	OT.Data_Authenticity	OT.Data_Confidentiality	OT.Data_Integrity	OT.Identification	OT.Prot_Abuse-Func	OT.Prot_Inf_Leak	OT.Prot_Malfunction	OT.Prot_Phys-Tamper	OT.Tracing	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.SCD_SVD_Corresp	OT.SCD_Unique	OT.SCD/SVD_Auth_Gen	OT.Sig_Secure	OT.Sigy_SigF	OT.Tamper_ID	OT.Tamper_Resistance	OT.TOE_TC_VAD_Imp	OT.TOE_TC_DTBS_Imp	OT.TOE_SSCD_Auth	OT.TOE_TC_SVD_Exp
FIA_UAU.1/UPD			X		X																															
FIA_AFL.1/Suspend_PIN_EAC2PP										X		X		X	X	X																				
FIA_AFL.1/Block_PIN_EAC2PP										X		X		X	X	X						X														
FIA_API.1/CA_EAC2PP											X	X		X	X	X																				
FIA_UID.1/PACE_EAC2PP												X		X	X	X																				
FIA_UID.1/EAC2_Terminal_EAC2PP										X		X		X	X	X																				
FIA_UAU.1/PACE_EAC2PP												X		X	X	X																				
FIA_UAU.1/EAC2_Terminal_EAC2PP										X		X		X	X	X																				
FIA_UAU.4/PACE_EAC2PP												X		X	X	X																				
FIA_UAU.5/PACE_EAC2PP												X		X	X	X																				
FIA_UAU.6/CA_EAC2PP												X		X	X	X																				
FIA_AFL.1/PACE_EAC2PP																						X														
FIA_UAU.6/PACE_EAC2PP												X		X	X	X																				
FIA_UAU.1/PACE_EAC1PP									X				X	X	X	X																				
FIA_UAU.4/PACE_EAC1PP									X				X	X	X	X																				
FIA_UAU.5/PACE_EAC1PP									X				X	X	X	X																				
FIA_UAU.6/PACE_EAC1PP														X	X	X																				
FIA_UAU.6/EAC_EAC1PP									X				X	X	X	X																				
FIA_API.1/EAC1PP								X																												
FIA_AFL.1/PACE_EAC1PP																						X														
FIA_UID.1/PACE_EAC1PP									X				X	X	X	X																				
FIA_UID.1/SSCDPP																													X		X					
FIA_AFL.1/SSCDPP																															X					
FIA_AFL.1/BIO_SSCDPP																															X					
FIA_API.1/SSCDPP4																																			X	
FIA_UAU.1/SSCDPP																													X		X					
FMT_SMR.1	X							X		X		X	X	X	X	X	X																			
FMT_LIM.1/Loader		X																																		
FMT_LIM.2/Loader		X																																		
FMT_SMF.1/UPD			X																																	
FMT_MTD.1/UPD_SK_PICC				X	X		X																													
FMT_MTD.1/UPD_KEY_READ				X	X		X																													
FMT_SMR.1/UPD				X	X																															
FMT_MTD.1/CVCA_INI_EAC2PP												X		X	X	X																				
FMT_MTD.1/CVCA_UPD_EAC2PP												X		X	X	X																				
FMT_SMF.1/EAC2PP										X		X		X	X	X	X																			
FMT_SMR.1/PACE_EAC2PP										X		X		X	X	X	X																			
FMT_MTD.1/DATE_EAC2PP												X		X	X	X																				
FMT_MTD.1/PA_EAC2PP										X	X	X		X	X	X																				
FMT_MTD.1/SK_PICC_EAC2PP											X	X		X	X	X																				
FMT_MTD.1/KEY_READ_EAC2PP										X	X	X		X	X	X																				
FMT_MTD.1/Initialize_PIN_EAC2PP										X		X		X	X	X																				
FMT_MTD.1/Change_PIN_EAC2PP										X		X		X	X	X																				
FMT_MTD.1/Resume_PIN_EAC2PP										X		X		X	X	X																				
FMT_MTD.1/Unblock_PIN_EAC2PP										X		X		X	X	X																				
FMT_MTD.1/Activate_PIN_EAC2PP										X		X		X	X	X																				
FMT_MTD.3/EAC2PP												X		X	X	X																				
FMT_LIM.1/EAC2PP																	X																			
FMT_LIM.2/EAC2PP																	X																			
FMT_MTD.1/INI_ENA_EAC2PP										X							X																			
FMT_MTD.1/INI_DIS_EAC2PP										X							X																			
FMT_SMF.1/EAC1PP								X					X	X	X	X	X																			
FMT_SMR.1/PACE_EAC1PP								X					X	X	X	X	X																			
FMT_LIM.1/EAC1PP																		X																		
FMT_LIM.2/EAC1PP																		X																		
FMT_MTD.1/INI_ENA_EAC1PP													X				X																			
FMT_MTD.1/INI_DIS_EAC1PP													X				X																			
FMT_MTD.1/CVCA_INI_EAC1PP									X																											
FMT_MTD.1/CVCA_UPD_EAC1PP									X																											
FMT_MTD.1/DATE_EAC1PP									X																											
FMT_MTD.1/CAPK_EAC1PP								X	X							X																				
FMT_MTD.1/PA_EAC1PP													X	X	X	X																				
FMT_MTD.1/KEY_READ_EAC1PP								X	X					X	X	X																				
FMT_MTD.3/EAC1PP									X																											
FMT_SMR.1/SSCDPP																									X					X						
FMT_SMF.1/SSCDPP																									X		X			X						
FMT_MOF.1/SSCDPP																									X					X						
FMT_MSA.1/Admin_SSCDPP																									X				X							
FMT_MSA.1/Signatory_SSCDPP																									X					X						
FMT_MSA.2/SSCDPP																									X				X	X						
FMT_MSA.3/SSCDPP																									X				X	X						
FMT_MSA.4/SSCDPP																									X		X		X	X						
FMT_MTD.1/Admin_SSCDPP																									X					X						
FMT_MTD.1/Signatory_SSCDPP																									X					X						
FPT_EMS.1/UPD							X																													
FPT_FLS.1/UPD						X																														
FPT_TST.1/UPD						X																														
FPT_EMS.1/EAC2PP																			X																	
FPT_FLS.1/EAC2PP																			X	X																
FPT_TST.1/EAC2PP																			X	X																
FPT_PHP.3/EAC2PP																X			X		X															
FPT_EMS.1/EAC1PP													X						X																	
FPT_TST.1/EAC1PP																			X	X																
FPT_FLS.1/EAC1PP																			X	X																
FPT_PHP.3/EAC1PP																X			X		X															
FPT_EMS.1/SSCDPP																							X				X									
FPT_FLS.1/SSCDPP																											X									
FPT_PHP.1/SSCDPP																																X				
FPT_PHP.3/SSCDPP																											X						X			
FPT_TST.1/SSCDPP																									X	X				X						
FTP_ITC.1/UPD			X		X																	X														
FTP_ITC.1/PACE_EAC2PP												X		X	X	X						X														
FTP_ITC.1/CA2_EAC2PP												X		X	X	X						X														
FTP_ITC.1/PACE_EAC1PP														X	X	X						X														
FTP_ITC.1/SVD_SSCDPP4																																				X
FTP_ITC.1/VAD_SSCDPP5																																		X		
FTP_ITC.1/DTBS_SSCDPP5																																			X	

Tabla 7.- Coverage of Security Objectives for the TOE by SFRs

The dependency analysis for the security functional requirements given in the corresponding Tables of the Protection Profiles, and the SFRs described in Chapter 7.1.1.5, shows that the mutual support and internal consistency between all defined.

7.3.2. Rationale for SFR's Dependencies

The dependency analysis for the security functional requirements shows that the basis for mutual support and internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed, and non-dissolved dependencies are appropriately explained.

The dependency analysis has directly been made within the description of each SFR in Section 6.1 above. All dependencies being expected by CC part 2 [CC] and by extended components definition in Chapter 5 are either fulfilled, or their non-fulfillment is justified.

7.3.3. Security Assurance Requirements Rationale

The current assurance package was chosen based on the predefined assurance package EAL4. This package permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level, at which it is likely to retrofit to an existing product line in an economically feasible way. EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security specific engineering costs.

The selection of the component ALC_DVS.2 provides a higher assurance of the security of the electronic document's development and manufacturing, especially for the secure handling of sensitive material.

The selection of the component ATE_DPT.2 provides a higher assurance than the predefined EAL4 package due to requiring the functional testing of SFR-enforcing modules.

The selection of the component AVA_VAN.5 provides a higher assurance than the predefined EAL4 package, namely requiring a vulnerability analysis to assess the resistance to penetration attacks performed by an attacker possessing a high attack potential. This decision represents a part of the conscious security policy for the electronic document required by the electronic document issuer and reflected by the current ST.

The set of assurance requirements being part of EAL4 fulfills all dependencies a priori. The augmentation of EAL4 chosen comprises the following assurance components: ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5. For these additional assurance component, all dependencies are met or exceeded in the EAL4 assurance package. Below we list only those assurance requirements that are additional to EAL4.

ALC_DVS.2

Dependencies:

None

ATE_DPT.2

Dependencies:

ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

fulfilled by ADV_ARC.1, ADV_TDS.3, ATE_FUN.1

AVA_VAN.5

Dependencies:

ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

fulfilled by ADV_ARC.1, ADV_FSP.4, ADV_TDS.3, ADV_IMP.1, AGD_OPE.1, AGD_PRE.1, ATE_DPT.2

7.3.4. Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) are internally consistent. The analysis of the TOE´s security requirements with regard to their mutual support and internal consistency demonstrates:

The dependency analysis in Section 6.3.2 for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analyzed and non-satisfied dependencies are appropriately justified.

All subjects and objects addressed by more than one SFR are also treated in a consistent way: the SFRs impacting them do not require any contradictory property or behavior of these ‘shared’ items.

The assurance package EAL4 is a predefined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in Section 6.3.3 shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements can only arise due to functional-assurance dependencies not being met. As shown in Section 6.3.2 and Section 6.3.3, the chosen assurance components are adequate for the functionality of the TOE. Hence, there are no inconsistencies between the goals of these two groups of security requirements.

8. Resumen de las características funcionales del producto

El TOE provee las siguientes capacidades relacionadas con las aplicaciones de firma electrónica, identificación electrónica y pasaporte electrónico:

1. Establecimiento del canal seguro

Para el establecimiento del canal seguro, en primer lugar, se realiza un intercambio de las claves públicas de la tarjeta y el terminal mediante certificados que serán verificados por ambas partes. A continuación se realiza un protocolo de autenticación mutua, con intercambio de semillas para la derivación de una semilla común que dé lugar a las claves de sesión de cifrado y autenticado.

Una vez concluido el protocolo para el establecimiento de la semilla común todos los mensajes deben transmitirse securizados.

Si se rompe el canal seguro establecido debido a que se haya recibido un comando APDU que no respete el formato de mensaje securizado o a que la información de autenticación o MAC sea errónea, el canal queda deshabilitado y el estado de seguridad de la tarjeta es reseteado (se borran las claves de sesión y los secretos presentados quedan invalidados).

Este procedimiento permite que cada una de las partes (tarjeta y aplicación externa) confíe en la otra, mediante la presentación mutua de certificados, y su verificación. En el proceso, también se incluye el intercambio seguro de unas claves de sesión, que deberán ser utilizadas para securizar (encriptar) todos los mensajes intercambiados posteriormente.

- Autenticación con intercambio de claves

  Este procedimiento corresponde con el apartado 3.9 del documento [EN419212-3], en el que se utilizan claves RSA de 3072 a 3840 bits, y SHA-256 en la validación de certificados y en los comandos de autenticación.

- Autenticación de dispositivo con protección de privacidad

  Este procedimiento corresponde con el apartado 3.6 del documento [EN419212-3], en el que se utilizan claves EC de 256 a 521 bits, y SHA-256 en la validación de certificados y en los comandos de autenticación.

- Protocolo EAC

  Este procedimiento corresponde con el apartado 3.7 del documento [EN419212-3] y con las especificaciones [TR03110-2], en el que se utilizan claves EC de 256 a 521 bits, y SHA-256 en la validación de certificados y en los comandos de autenticación.

  Las aplicaciones eSign y eID soportan EAC2, es decir, Chip Authentication versión 2 y Terminal Authentication versión 2. Mientras que la aplicación ePass soporta tanto

EAC1, es decir, Chip Authentication versión 1 y Terminal Authentication versión 1 como EAC2.

- Protocolo PACE

Es un protocolo Diffie-Hellman key agreement que se basa en una contraseña (MRZ, CAN, PIN o PUK) definido en [TR03110-2]. Se debe establecer antes de cualquier otro canal para acceder a las aplicaciones del TOE. También es utilizado como canal seguro en la verificación del PIN en la aplicación eSign.

El TOE soporta la versión 2 de PACE según [TR03110-1], con el algoritmo ECDH AES 192 con curvas de 256 bits, 384 bits, 512 bits y 521 bits.

Esta alternativa se basa en la capacidad de la tarjeta para verificar certificados firmados por una autoridad certificadora raíz, posiblemente a través de autoridades certificadoras intermedias, y en la comprobación mediante protocolos de desafío-respuesta de que la otra parte dispone de la clave privada asociada al certificado.

Cuando se completa con éxito el establecimiento de un canal seguro, se adquiere un nuevo estado de seguridad en el diálogo con la tarjeta, que en función del certificado utilizado por el terminal, podrá ser:

- Canal Seguro Administrativo. Corresponde a la condición de acceso “PRO”, y por lo tanto se podrá acceder a los recursos que requieran esta condición. Solamente se puede establecer con los canales Autenticación con intercambio de claves o Autenticación de dispositivo con protección de privacidad definidos en [EN419212-3].

- Canal Seguro de Usuario. Se corresponde con el canal EAC2 definido en [TR03110-2].

- Canal Seguro de PIN. Se emplea para la presentación de los códigos CHV. Necesario como paso previo a la realización de la operación de firma. Se corresponde con el canal PACE definido en [TR03110-2].

2. Securización de mensajes

El TOE puede, previo establecimiento de un canal seguro, securizar los mensajes transmitidos. Para el establecimiento es necesaria la autenticación previa del terminal y la tarjeta, mediante el uso de certificados electrónicos.

Cuando el canal está establecido, los mensajes intercambiados entre la tarjeta y terminal se cifran y autentican, de tal forma que se asegura una comunicación una-a-uno entre los dos puntos originarios de canal. El canal seguro puede ser requerido por la aplicación o puede ser una restricción de acceso impuesta a algún recurso de la tarjeta.

3. Identificación y Autenticación

El TOE dispone de distintos métodos de autenticación, mediante los que una entidad externa demuestra su identidad, o el conocimiento de algún dato secreto almacenado en la tarjeta.

La correcta realización de cada uno de estos métodos, permite obtener unas condiciones de seguridad, que podrán ser requeridas para el acceso a los distintos recursos de la tarjeta.

- Autenticación de usuario mediante PIN

La tarjeta soporta verificación de usuario (CHV- Card Holder verification) para el acceso a determinados ficheros. La verificación es realizada, a través del canal seguro de PIN, comprobando el código facilitado por la entidad externa a través del comando diseñado para tal fin. El dato es comparado con la información de referencia almacenada en el fichero CHV. El código CHV (PIN) es una secuencia de 12-16 bytes.

Cada código CHV tiene su propio contador de intentos. Tras una presentación válida de PIN, el contador de reintentos correspondiente es automáticamente puesto a su valor inicial (3 intentos). El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Es posible desbloquear un código CHV tras una correcta presentación del código de desbloqueo. La operación de desbloqueo se realiza con la autenticación de usuario mediante biometría y la presentación de la clave “APP”.

- Desbloqueo de PIN (Condición 1: Biometría)

La tarjeta DNIe tiene soporte para biometría con algoritmo “Match on Card”, es decir, la verificación de los datos biométricos frente a los datos de referencia se realiza dentro de la propia tarjeta. Por tanto, se mantienen los datos sensibles de biometría siempre internos a la tarjeta, y su utilización está controlada mediante control de acceso. Esta característica de “Match on Card” confiere una importante diferencia frente a algoritmos “Match off Card”, donde la tarjeta sólo es utilizada como soporte de los datos para la verificación externa.

La autenticación del usuario con técnicas biométricas permite, junto con la “clave APP”, desbloquear el código CHV y establecer un nuevo valor. La biometría también es necesaria para realizar la solicitud o renovación de los certificados de firma y autenticación. La autenticación biométrica se realiza bajo un canal seguro de administrador.

En lo relativo a la autenticación del usuario por biometría, la tarjeta DNIe almacena 2 huellas dactilares.

Una ronda fallida de presentación de huella se compone de tres intentos fallidos de presentación de la huella de una mano más tres intentos fallidos de presentación de la huella de la otra mano.

Cada ronda fallida de presentación de huella obliga a la extracción de la tarjeta. Cuatro rondas fallidas bloquean el mecanismo de presentación de huella en su conjunto.

- Desbloqueo de PIN (Condición 2: clave APP)

El propósito de este método de autenticación es que la entidad externa demuestre tener conocimiento del nombre y valor de un código secreto. Este código, al que denominaremos como "clave APP", normalmente residirá en una tarjeta porta-claves, y nunca estará en claro fuera de un dispositivo seguro.

Cada clave APP tiene su propio contador de intentos. Tras una presentación válida, el contador de reintentos correspondiente es automáticamente puesto a su valor inicial (3 intentos). El contador de intentos es decrementado cada vez que se realiza una presentación errónea, pudiendo llegar a bloquearlo si el contador llega a cero. Si este código llega a bloquearse no será posible realizar la operación de desbloqueo.

Esta clave APP junto con la autenticación de usuario mediante biometría permite desbloquear el código CHV del usuario. La operación se realiza mediante el uso de un canal seguro de administrador.

4. Opciones del TOE – Biometría y actualización de S.O.

- Biometría

El TOE dispone de un método de autenticación basado en la identificación biométrica "Match On Card". Este mecanismo es suministrado por dos proveedores diferentes con objeto de reducir la dependencia tecnológica de cada uno de ellos. Ambos proveedores ofrecen prestaciones equivalentes tanto en rendimiento como en las diferentes tasas de comparación biométrica. Se procura que la mitad de los TOE cuenten con la biometría de un proveedor y la otra mitad de los TOE con la biometría del otro con objeto de tener un reparto equilibrado.

- Actualización de Sistema Operativo

El TOE cuenta con un mecanismo que permite la actualización del sistema operativo en el caso de que se considere necesario. Si este mecanismo se encuentra activo, en dicha opción del TOE aplicarían los SFR relacionados con esta funcionalidad. Concretamente: FCS_COP.1.1/UPD_ITC, FCS_CKM.1.1/UPD_ITC, FCS_COP.1.1/UPD_DEC, FCS_CKM.1.1/UPD_DEC, FCS_COP.1.1/UPD_SIG, FCS_COP.1.1/UPD_INT, FCS_CKM.1.1/UPD_INT, FCS_CKM.4.1/UPD, FCS_CKM.4.1/UPD_OS, FIA_AFL.1.1/UPD, FIA_AFL.1.2/UPD, FIA_UID.1.1/UPD, FIA_UID.1.2/UPD, FIA_UAU.1.1/UPD, FIA_UAU.1.2/UPD, FDP_ACC.1.1/UPD, FDP_ACF.1.1/UPD, FDP_ACF.1.2/UPD, FDP_ACF.1.3/UPD, FDP_ACF.1.4/UPD, FDP_IFC.1.1/UPD, FDP_IFF.1.1/UPD, FDP_IFF.1.2/UPD, FDP_IFF.1.3/UPD, FDP_IFF.1.4/UPD, FDP_IFF.1.5/UPD, FDP_RIP.1.1/UPD, FTP_ITC.1.1/UPD, FTP_ITC.1.2/UPD, FTP_ITC.1.3/UPD, FAU_SAS.1.1/UPD, FMT_SMF.1.1/UPD, FMT_MTD.1.1/UPD_SK_PICC, FMT_MTD.1.1/UPD_KEY_READ, FMT_SMR.1.1/UPD, FMT_SMR.1.2/UPD, FPT_EMS.1.1/UPD, FPT_EMS.1.2/UPD, FPT_FLS.1.1/UPD, FPT_TST.1.1/UPD, FPT_TST.1.2/UPD, FPT_TST.1.3/UPD, FMT_LIM.1.1/Loader y FMT_LIM.2.1/Loader.

Si el mecanismo no se encuentra activo, a dicha opción del TOE no le aplicarían los SFRs mencionados anteriormente.

9. Acrónimos

ALC	Clase Life-Cycle Support
APDU	Application Protocol Data Unit, Unidad de Datos del Protocolo de Aplicación
ATS	Answer To Select, Respuesta al comando Select ISO 14443-4
BAC	Basic Access Control
BIS-BAC	Basic Inspection System with BAC
CA	Autoridad de Certificación
CA2	Chip Authentication 2
CAN	Card Access Number
CC	Common Criteria
CGA	Certificate-generation application, Aplicación de Generación de Certificados
CHAT	Certificate Holder Authorization Template
CPU	Central Processing Unit, Unidad Central de Proceso
CRT	Chinese Remainder Theorem, Teorema del Residuo Chino
CSP	Certification Service Provider, Proveedor de Servicios de Certificación
DEMA	Differential Electromagnetic Analysis
DES	Data Encryption Standard
DNIe	Documento Nacional de Identidad Electrónico
DPA	Differential Power Analysis
DTBS	Data to be signed, Datos a ser firmados
DTBS/R	Data to be signed or its unique representation, Representación unívoca de los datos a ser firmados
EAC	Extended Access Control
EAL	Evaluation Assurance Level, Nivel de garantía de evaluación
ECC	Elliptic curve cryptography, Criptografía de curvas elípticas
EEPROM	Electrically Erasable Programable Read Only Memory, Memoria ROM programable eléctricamente
FDP	User Data Protection, Protección de datos de usuario
FIPS	Federal Information Processing Standard
GND	Ground, Tierra
HI	Human Interface, Interfaz humana
IC	Integrated Circuit, Circuito Integrado

ICAO	International Civil Aviation Organization
IO	Input/Output, Entrada/Salida
ISO	International Organization for Standardization
MRZ	Machine Readable Zone
MSE	Manage Security Environment
OS	Operating system, Sistema Operativo
OSP	Organizational security policy
PACE	Password Authenticated Connection Establishment
PKCS	Public Key Cryptography Standards, Normas de Criptografía de Clave Pública
PIN	Personal Identification Number, Número de Identificación Personal
PP	Protection Profile, Perfil de Protección
PUK	PIN Unblocking Key, Clave de Desbloqueo del PIN
RAD	Reference authentication data, Datos de referencia de autenticidad
RAM	Random Access Memory, Memoria de acceso aleatorio
ROM	Read Only Memory, Memoria de solo lectura
RSA	Rivest, Shamir & Adleman
SAC	Supplemental Access Control
SCA	Signature Creation Application, Aplicación de creación de firma
SCD	Signature Creation Data, Datos de creación de firma
SDO	Signed Data Object, Objeto de datos firmado
SFP	Security Function Policy, Política de función de seguridad
SFR	Security Functional Requirement, Requisito funcional de seguridad
SHA	Secure Hashing Algorithm
SPA	Simple Power Analysis
ST	Security Target, Declaración de Conformidad
SVD	Signature Verification Data, Datos de verificación de firma
TA	Terminal Authentication
TOE	Target of Evaluation, Objeto a evaluar
TSF	TOE Security Functionality, Funciones de seguridad del TOE
TSFI	TSF Interface, Interfaz de las funciones de seguridad del TOE
VAD	Verification Authentication Data, Datos de verificación de identidad
VCC	Supply Voltage, Tensión de Alimentación

10. Bibliografía

[AGO] Anexo I Ejemplo - Guía Operativa para usuario final. DNIe 4.01. v.1.0. r.0. 20/05/2024.

[NIST SP 800-90A] NIST Special Publication 800-90A Revision 1, Recommendation for Random Number Generation Using Deterministic Random Bits Generators, June 2015.

[AES] Federal Information Processing Standards Publication 197 Advanced Encryption Standard. U.S. Department of Commerce/National Institute of Standards and Technology, 2001 November 26.

[ANSI X9.62] Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA). American National Standards Institute, ANSI, 2005.

[ANSI X9.63] Public Key Cryptography for the Financial Services Industry - Key Agreement and Key Transport Using Elliptic Curve Cryptography. American National Standards Institute, ANSI, 2001.

[ASE_COMP] Composite product evaluation for smart card and similar devices, v1.5.1, May. 2018.

[BACPP] Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application", Basic Access Control, BSI-CC-PP-0055-2009, Version 1.10, 25th March 2009.

[CC] Common Criteria for Information Technology Security Evaluation. April 2017. Version 3.1. Revision 5.

[CMD] Especificación funcional. Manual de comandos. DNIe 4.01. v.1.0. r.0. 20/05/2024.

[eIDAS] Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

[EN419212-3] EN 419212-3. Interfaz de aplicación para tarjetas inteligentes utilizadas como dispositivos seguros de creación de firma. Parte 3: Protocolos de autentificación de dispositivos. Noviembre 2017.

[DIR] Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica.

[DE] Decisión de ejecución (UE) 2016/650 de la Comisión de 25 de abril de 2016 por la que se fijan las normas para la evaluación de la seguridad de los dispositivos cualificados de creación de firmas y sellos con arreglo al artículo 30, apartado 3, y al artículo 39, apartado 2, del Reglamento (UE) n.o 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

[EAC1PP] Common Criteria Protection Profile — Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), ver. 1.3.2, 05th December 2012, BSI-CC-PP-0056-V2-2012.

[EAC2PP] Common Criteria Protection Profile — Electronic document implementing Extended Access Control Version 2 (EAC2) defined in BSI TR-03110 (EAC2_PP), ver. 1.01, May 20th, 2015, BSI-CC-PP-0086.

[FIPS 140-2] Security Requirements for Cryptographic Modules, National Institute of Standards and Technology (NIST), up to change notice December 3, 2002

[FIPS 186-4] Digital Signature Standard (DSS) July 2013.

[GO] Guías Operativas. DNIe 4.01. v.1.0 r0. 20/05/2024.

[GOA] Guía operativa para administrador. DNIe 4.01. v.1.0. r.0. 20/05/2024.

[GOU] Guía Operativa para usuario final. DNIe 4.01. v.1.0. r.0. 20/05/2024.

[GP] Guía preparativa. DNIe 4.01. v.1.0. r.0. 20/05/2024.

[ICAO9303] International Civil Aviation Organization, ICAO Doc 9303, Machine Readable Travel Documents – Machine Readable Passports, Version Seventh Edition, 2015.

[ICAO-SAC] ICAO: Technical Report: Supplemental Access Control for Machine Readable Travel Documents, Version - 1.01, 11. November 2010.

[ICPP] Inside Secure, Infineon Technologies AG, NXP Semiconductors Germany GmbH, STMicroelectronics: Common Criteria Protection Profile - Security IC Platform Protection Profile with Augmentation Packages, BSI-CC-PP-0084-2014, v1.0. 13 January 2014.

[ISO7816-2] ISO/IEC 7816 Identification cards -- Integrated circuit cards -- Part 2: Cards with contacts -- Dimensions and location of the contacts. 2007.

[ISO7816-4] Identification cards -- Integrated circuit cards -- Part 4: Organization, security and commands for interchange. 2005.

[ISO11770-3] ISO/IEC 11770-3 Information technology -- Security techniques -- Key management – Part 3: Mechanisms using asymmetric techniques

[ISO15946-1] ISO/IEC 15946-1 Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General. 2002.

[MR2] Assurance Continuity Maintenance Report. BSI-CC-PP-0059-2009-MA-02. 30/06/2016.

[MR4] Assurance Continuity Maintenance Report. BSI-CC-PP-0071-2012-MA-01. 30/06/2016.

[MR5] Assurance Continuity Maintenance Report. BSI-CC-PP-0072-2012-MA-01. 30/06/2016.

[MR.ED-PP] Common Criteria Protection Profile — Machine-Readable Electronic Documents based on BSI TR-03110 for Official Use, BSI-CC-PP-0087-V2-MA-01, Version 2.0.3, July 18th, 2016.

[MR.ED-ON-PP] Common Criteria Protection Profile - Configuration Machine Readable Electronic Documents - Optionales Nachladen (Optional Post-Emission Updates), BSI-CC-PP-0090-2016, Version 0.9.2, August 18th, 2016.

[NIST SP 800-186] Recommendations for Discrete Logarithm_Based Cryptography: Elliptic Curve Domain Parameters

[PACEPP] Common Criteria Protection Profile — Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.01, 22th July 2014, BSI-CC-PP-0068-V2-2011-MA-01.

[PKCS#1] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1.

[RFC5639] M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, IETF, 2010-03.

[SSCDPP] Protection profiles for secure signature creation device — Part 2: Device with key generation, prEN 14169-2:2012 ver. 2.0.1, 2012-01, BSI-CC-PP-0059-2009-MA-01.

[SSCDPP4] Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application, prEN 14169-4:2012 ver. 1.0.1, 2012-11, BSI-CC-PP-0071.

[SSCDPP5] Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted communication with signature creation application. prEN 14169-5:2012 ver. 1.0.1, 2012-11, BSI-CC-PP-0072.

[SHS] Federal Information Processing Standards Publication 180-4 Secure Hash Standard, U.S. Department of Commerce/National Institute of Standards and Technology, March 2012.

[TR03110] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Parts 1, 2 and 3. See more details below.

[TR03110-1] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1. Version 2.20. 26. February 2015

[TR03110-2] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 2: Protocols for electronic IDentification, Authentication and trust Services (eIDAS). Version 2.21. 21. December 2016.

[TR03110-3] Technical Guideline TR-03110. Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3: Common Specifications. Version 2.21. 21. December 2016.

[TR03111] BSI: TR 03111: Elliptic Curve Cryptography, Version 2.0, 28. June 2012.

[TR03116-2] BSI: TR 03116-2: Kryptographische Vorgaben für Projekte der Bundesregierung Teil 2 – Hoheitliche Ausweisdokumente, 2. February 2015

11. Índice de tablas